T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
IŞLETME ANABİLİM DALI
YÖNETİM VE ORGANİZASYON (İNGİLİZCE) BİLİM DALI

ENTERPRISE RISK MANAGEMENT IN TELECOMMUNICATION INDUSTRY IN TURKEY:

A FRAMEWORK SET-UP AND IMPLEMENTATION

Yüksek Lisans Tezi

SÜLEYMAN SERDAR SEYHANLI

İstanbul, 2010

T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
IŞLETME ANABİLİM DALI
YÖNETİM VE ORGANİZASYON (İNGİLİZCE) BİLİM DALI

ENTERPRISE RISK MANAGEMENT IN TELECOMMUNICATION INDUSTRY IN TURKEY:

A FRAMEWORK SET-UP AND IMPLEMENTATION

Yüksek Lisans Tezi

SÜLEYMAN SERDAR SEYHANLI

DANIŞMAN: Doç.Dr.ASLI KÜÇÜKASLAN

İstanbul, 2010

Marmara Üniversitesi
Sosyal Bilimler Enstitüsü Müdürlüğü

Tez Onay Belgesi

İŞLETME Anabilim Dalı YÖNETİM VE ORGANİZASYON(İNG) Bilim Dalı Yüksek Lisans öğrencisi SÜLEYMAN SERDAR SEYHANLI nın ENTERPRISE RISK MANAGEMENT IN TELECOMMUNICATION INDUSTRY IN TURKEY: A FRAMEWORK SET - UP AND IMPLEMENTATION adlı tez çalışması ,Enstitümüz Yönetim Kurulunun 25.01.2010 tarih ve 2010-1/26 sayılı kararıyla ile oluşturulan jüri tarafından oy birliği / oy çokluğu ile Yüksek Lisans Tezi olarak kabul edilmiştir.

	Öğretim Üyesi Adı Soyadı	**İmzası**
Tez Savunma Tarihi	: 10/6/2010	
1) Tez Danışmanı :	**DOÇ. DR. FATMA ASLI KÜÇÜKASLAN**	.....
2) Jüri Üyesi :	**PROF. DR. FATMA GÜLRUH GÜRBÜZ**	.....
3) Jüri Üyesi :	**YRD. DOÇ.DR. SADULLAH ÇELİK**	.....

CONTENTS

ABSTRACT

ENTERPRISE RISK MANAGEMENT IN TELECOMMUNICATION INDUSTRY IN TURKEY: A FRAMEWORK SET-UP AND IMPLEMENTATION

In recent years, the focus on risk management increased significantly and has become an evident the need for companies to have a good reference model to identify, measure and evaluate uncertain events that affect the organization.
The risk, complexity and uncertainty have become factors that inevitably characterize the environment in which each company operates. The increasing competitiveness, globalization of markets, regulatory changes, new technologies, customer expectations, which change rapidly, have helped increase the focus on risk management, raising the need to improve systems internal control of companies to try to anticipate and manage change and uncertainty in order to strengthen and enhance its ability to create value for the various categories of stakeholders. Therefore, "Risk Management" became a process to be combined with other processes in the company to govern more effectively and efficiently the entire organization.

The aim of this study is to examine the existing enterprise risk management structures within four Telecommunication companies in Turkey, their effectiveness within the organization, integration with business processes, current and expected future benefits of risk management systems. This thesis would be a useful support for companies wishing to approach the topic of Risk Management, to improve their strategic process, exploiting the opportunities arising quickly by the high uncertainty characterizing the current competitive environment. Through out this study, I had tried to identify not only the benefits but also the limitations and challenges of effective risk management strategy for Telecom Industry which is comparatively new and exciting market in Turkey. The initial section of the study covers the theoretical background of enterprise risk management and summarizes various risk management standards applied in the world together with implementation alternatives. The later section presents the analysis of a questionnaire conducted in the Turkish Telecom sector offering a maturity assessment of existing applications of enterprise risk management in Turkey.

Keywords: Enterprise Risk Management, Risk Assessment, Telecommunications, Internal Audit

LIST OF TABLES

Page No

LIST OF FIGURES

Page No

ABBREVIATIONS

ERM Enterprise Risk Management

COSO Committee of Sponsoring Organizations

MIS Management Information Systems

SOX Sarbanes Oxley Act

GARP Generally Accepted Risk Principles

AS/NZS Australian / New Zealand Risk Management Framework

CSF Critical Success Factors

KPI Key Performance Indicators

RFI Production of a Request for Information

SAS 70 Statement on Auditing Standard

IT Information Technologies

1. INTRODUCTION

Risk is an integral part of today's modern management. By carrying out risk management in a more consistent and structured way, management becomes more effective. Most risk management systems aim to avoid risk but, if a business doesn't take risks, it can't grow. The Telecommunications industry is evolving rapidly as triggered by technological developments and by changes in the competitive and regulatory environment. It is not only the shifting technological trends but also the economic instability that affects the companies and makes enterprise-wide risk management a "necessity" for sustainable growth

The aim of this study is to understand and evaluate the existing risk management dynamics in local Telecommunications market which is a very important industry worldwide. Based on the previous literature review, it important to note that telecommunications industry is about a $3.5 trillion sector only in United States and have more than 2.3 billion cell phone service subscribers worldwide. (Becheer Carlson, 2010). According to the statistics, mobile cellular subscriptions had been tripled between 2003 and 2009 in Turkey, which affected the fixed line usage as well (ITU World Telecommunication, 2009). The current global economic crisis affects the companies all, not only bring additional risks but bring opportunities for the industry as well existing competitors in the market are facing various opportunities as a result of these developments, but also facing threats. In this context, traditional revenue streams are getting narrow due to increased competition and customer transfers between Telecommunication companies. The power of the regulatory bodies in Turkey is increasing by each day and they have a significant impact on the possibility of certain operators to compete effectively. Unstable economic environment creates significant risks, not only for the Telecommunication companies but also for the all stakeholders in the market such as banking and insurance. Companies that are not able to implement effective means of risk management tend to face bankruptcy such as Lehman Brothers, but some who suffered

seriously from previous crisis were able to survive, such as the players of Turkish banking industry.

The importance of this study is to not only to highlight the key elements of enterprise risk management but also to present outcomes and how the companies should perceive these risks. Therefore the rationale is built on tailoring an enterprise risk management methodology for "Telecommunications Industry" which enriched with up-to-date examples from all players in Turkish market in addition to research conducted to investigate and evaluate the existing risk management structures and maturity levels of Telecom companies.

1. THE LITERATURE REVIEW

The purpose of this literature review is to compile and summarize information related to enterprise risk management to support the development risk management framework and guidelines for efficient implementation in Telecommunication companies. This review specifically focused on information, themes and important aspects of the following elements of risk management:

- Definition of risk
- Concept of risk analysis and management
- Purpose of enterprise risk management and how to implement it in Telecommunications industry and,
- Application of Committee of Sponsoring Organization's (COSO) framework for enterprise risk management implementation.

In order to accomplish this review, a selection of key documents about risk management was reviewed. In the academic and industrial circles there is huge amount of

generic literature on risk nevertheless there is almost limited work on efficient or workable risk management methodologies that could be used by high-tech organizations such as Telecom companies. Therefore, selection of the review documents for this study was based on; (1) the quality and recentness of the content; (2) practicality and relevance to the Telecommunications industry; and (3) the credibility, reputation, and affiliation of the author(s) or the publishing organizations.

In recent years, enterprise risk management (ERM) has received unprecedented international and local attention. Many organizations shifted their traditional approached to risk to enterprise wide and interconnected risk management approach (Lam, 2000; Liebenberg and Hoyt, 2003). This transformation not only changed the route of academic and business-wise studies but also pointed to the lack of guidelines or common references for the new concept of risk management. The lack of a widely accepted ERM conceptual framework led the Committee of Sponsoring Organizations (COSO), widely known for its Internal Control Integrated Framework (COSO, 1992), to initiate an effort to develop common terminology and an accepted framework for ERM. In September 2004, COSO (2004) issued Enterprise Risk Management Integrated Framework that provides a model of the ERM process and defines ERM basics concepts. COSO ERM framework constitutes general guidelines for the theoretical framework of this study and was taken as bible for a successful ERM implementation for Telecom industry. Besides this framework review, practical COSO ERM application in Turkish Ministry of Finance which is performed by Chairmanship of Strategy Development had been reviewed as case study as well. (Ahmet Uğur Cebeci, Işılda Arslan, 2008)

Based on the previous literature review, it was observed that transformation in risk management approaches not only effected the academic and professional publications and studies, but also had great influence on many of the organizational roles especially in Internal Audit. Institute of Internal Auditors (2004) has issued guidance on internal audit's proper role in ERM. Two recent studies (Beasley et al.,2005a; Gramling and Myers, 2006)

have examined internal audit's role in ERM at a micro-level which will be discussed under an individual title within this study.

The "research methodology" section of this study is mainly based on the literature review of risk management survey and empirical studies of Mark S. Beasley and his team in North Carolina State University. Two of his studies "Enterprise risk management: An empirical analysis of factors associated with the extent of implementation" in 2005 and "The Information Conveyed in Hiring Announcements of Senior Executives Overseeing Enterprise-Wide Risk Management Processes" in 2006 had been used as a reference point for research methodology development. I have also utilized relevant and applicable parts of the published survey of Şule Güneş and Suat Teker : "Enterprise Risk Management Awareness in Turkish Energy Sector, 2010" and adopted for Telecommunications industry.

1.1. THE CONCEPT OF RISK ASSESSMENT

The Communication Sector is one of the areas which, over the past several years, evolved most significantly and caused revolutions in both system-wide and system-use aspects. These revolutions have resulted in many communication networks being set up without adequate consideration of the risks involved. Today, increasingly complex and IT-dependent digital elements (computers, networks, contents, etc.) or infrastructures are at the center of our lives; they constitute the essential pillars of our communication, economic, social and institutional infrastructures. (Gwendal Le Grand, Eyal Adar, 2007)

Risk assessment is therefore an essential stake in many industries, and it remains a burden because of its complexity. Actually, it is necessary to adopt a global vision that takes into account not only, identifying risks but analyzing them to assess the impacts on the business or on the corporate image of a company.

The existing risk management concepts are high level, mostly adopted from banking and insurance industry, not totally fit to cope with the specific needs and risks of the communication world. If the companies are able to define the specific elements which need to be examined while assessing the risks to communication systems, and define how proper risk assessment can aid in the process successful enterprise wide risk management.

In order to adapt these frameworks towards a more practical application for the telecom world, a layer of additional analysis is needed; such a layer must rely upon a thorough and multi-staged understanding of the telecom world's unique business needs and requirements, and its specific systems and procedures.

2.1.1 THE DEFINITION OF RISK ASSESSMENT

"Risk is the possibility that an event will occur and adversely affect the achievement of objectives."(The Committee of Sponsoring Organizations, 2004). Risk management begins with the through definition of what is risk and how risk assessment should be performed. Risk assessment forms the touchstone of an effective enterprise risk management program. Risk assessment is a mechanism for identifying which risks and related threats lies within. If performed properly, a risk assessment gives organizations a clear view of traps to which they may be exposed, whether internal or external, in addition to the opportunities attached as well. A good assessment is based on how the organizations define risk appetite and tolerance levels, which then provides a solid basis for determining risk responses that should be given to those risks. A good risk assessment process is directly tied to an organization's culture, applied consistently throughout the whole organization, empowers management to better identification and evaluation of the right risks for their business. This will be the basis for their decision making process whether they will accept those risk and maintain the appropriate controls to ensure effective and efficient operations, or mitigating them, transferring them to third parties or totally avoiding them.

A risk assessment should begin and end with specific business objectives that are tied with key value drivers. Business objectives of a company provide the basis for measuring the impact and probability of risk ratings. Corporate governance over the assessment process should be clearly established to feed up a comprehensive approach and a portfolio view, it should effectively facilitate the responses based on risk ratings and the organization's overall risk appetite and tolerance levels. With these basic but crucial principles, the risk assessment process should be aligned with the organization's business behavior and culture, periodically refreshed to catch up with the external and internal changes (Kleffner, 2003).

2.1.2 THE METHOD TO IDENTIFY AND ANALYZE RISK

Risk assessment can be done at different levels of the organization. It can be limited to a single risk type or a group of risks e.g. Environmental Risk / Health and Safety/ "Radiation Levels of Base Stations in Residential" Areas as a single risk or just Technological Risk as a main group. Risk assessment allows an entity to consider the extent to which potential events have an impact on achievement of objectives. Management assesses events from two perspectives - likelihood and impact - and normally uses a combination of qualitative and quantitative methods (World Intellectual Property Organization, 2004). Risk assessment criteria to determine likelihood and impact should be specially tailored for a company itself. As the industries, nature of the business, financial figures etc differ from one company to another, risk measurement and assessment techniques must be also different.

Table 1 A and B below represent the risk measurement scales for a local Telecom company. Table 1 A display the frequency that an adverse event will occur, which means the likelihood that a risk occurs actually and given a frequency number. Frequency type 1: "Once a year or more than a year" may be e.g. an environmental disaster and frequency 5: Daily or multiple times per day may be an event e.g. erroneous issuance of an mobile

subscriber's invoice. It should be kept in mind that, frequencies are only the likelihoods by not the severity of a damage that may occur.

Table 1 B is tabular presentation of impact levels matching with different levels of frequencies. Red, orange, yellow and green represents how critic the risk is and how immediate an action should be taken to manage it. If a frequency is high, which means that likelihood of a risk will occur is "high" and if its matching impact level is also high, there is an emergency situation that management needs to take serious actions for this risk group or the individual risk itself.

Bottom part of Table 1 B presents the different risk categories that Risk Committee of this Telecommunication Company evaluated beforehand. These categories can be renamed or diversified, which depends on the priorities of management. Categories in Table 1 B are as follows; Financial (financial losses or misstatements), Availability (availability of services, business continuity/interruption), Reputation, Clients (e.g. Loss of a client group or a whole segment) and Legal (case courts or penalties). It is possible to observe from that table that, those risk categories are somehow interrelated and their degree of severity differ as their level of impact increases. **Table 1 A&B**

Risk Measurement Scales

	A - Adverse event will occur
	Once a year or more than a year
	Between once a year and once a quarter
	Monthly
	Weekly
	Daily or multiple times per day

Source: Turkish Telecom Risk Assessment Workshop,2009

Likelihood	B – Impact				
	1	2	3	4	5
5	**Moderate**	**High**	**High**	**Very High**	**Very High**
4	**Moderate**	**Moderate**	**High**	**High**	**Very High**
3	**Low**	**Moderate**	**Moderate**	**High**	**High**
2	**Low**	**Low**	**Moderate**	**Moderate**	**High**
1	**Low**	**Low**	**Low**	**Moderate**	**Moderate**

	Financial	Availability	Reputation	Clients	Legal
1	impact <%0.01 impact < 800.000 TL	Business service interruption without effect or not visible for client without prior communication	Some confidential information (e.g. incidents, risk, ….) is known by management only	Loss of one or two mass market clients with complaints to other organizations	Occasional non-compliance with particular regulations with external impact
2	%0.01 <impact < %0.1 800.000 TL <impact < 8m. TL	Business service interruption, visible for client, however still with minimum services	Some confidential information is known by organisation and directly involved parties (banks, international organizations, regulator, …)	Loss of a limited number of mass market clients	Non-compliance with legislation, however the situations can easily be rectified. Contracts with unclear clauses.
3	%0.1 <impact < %1	Local / partially or National interruption of	Investigation of legislative	Loss of a significant number of mass market	Continuous non-compliance with a specific law / legislation

	8m. TL <impact < 80m. TL	business services, however still within the fixed RTO (Recovery Time Objective)	organizations	clients or loss of a limited number of « Large Accounts »	
4	%1 <impact < %5 80m. TL <impact < 400m. TL	Local / partially interruption of business services, outside de boundaries of the fixed RTO (Recovery Time Objective)	Article in the press (specialized press, general press, TV)	Loss of a "Key Account"	Continuous non-compliance with a specific law / legislation for which the organisation does not take action to rectify the situation, with an official investigation as a consequence
5	impact >%5 impact > 400m. TL	National interruption of services, outside de boundaries of the fixed RTO (Recovery Time Objective)	Continuous comments in the media with impossibility to change the public / shareholders / press opinion. Rupture with shareholders.	Loss of a entire segment / sector	Important relations are not formalized in a clear contract. Potential sentence and penalty by a (international/national) court with regard to the conformance of the activities of the organisation.

Source: Turkish Telecom Risk Assessment Workshop,2009

The most important point is that; all positive and negative impacts of potential events should be examined, individually or by category, across the entity. Risks should be assessed on both an inherent (before risk responses) and a residual basis (after risk response) and management should keep in mind that, risk assessment will be successful as

long as it covers all areas of risks that a company may experience. Referring to our risk table above, it is clear that management did not focused on risks regarding Health and Safety, Political, Socio-Economic and Technological Changes which can seriously harm the business when ignored.

2.1.3 TYPES OF RISK ASSESSMENT

There are different types of risks that reside in companies' risk portfolio and each should be managed with different strategy and by different levels of management within the organization. The different types of risk assessments can be listed as below (Kent D. Miller, 1992)

• *Strategic risk assessment:* Evaluation of risks relating to the organization's vision, mission statement and strategic objectives. As the corporate strategy is defined and managed at the top, this type of assessment should be performed with senior management. For Telecommunication industry, taking into consideration that most of the players in Turkish market are a part of joint venture or Group Company, Board of Directors or Risk Committee of Senior Managers should also be included to this type of assessment. This type of assessment is the touchstone of ERM Framework Development and should be performed for all ERM implementation projects. As the business strategy differs from one industry to another, strategic risks are also diversified. Table 2 lists the top ten strategic risks for Telecommunication industry for European Telecom Companies (Earnst and Young, 2009).

Table 2
Top Ten Strategic Telecommunication Risks in Europe

1. Decline in fixed and mobile voice ARPU
2. Failure to Generate sustainable cash flows for new business models
3. Inaccuracy to forecast returns from infrastructure investments
4. Technological shifts
5. Regulatory Risks
6. Competition from internet companies
7. Globalization of markets and services
8. Consolidation and M&A
9. Privacy and security risks
10. Inappropriate process and systems to support new business strategies

Source: Earnst and Young, Oxford Analytica, Telecommunication Business Risk Report, 2009, pg 12

• *Operational risk assessment.* This type of assessment is a level lower than the strategic risk assessments. Operational risk assessment is the evaluation of the potential risks of loss resulting from ineffective internal business processes, people, and systems, or from external events that could not be foreseen or ignored before. (Banham, R, 2004).

• *Compliance risk assessment.* There are risks resulting from an organization's compliance obligations, such as alignment with related laws and regulations, internal policies and procedures, general and corporate ethics rules, code of conduct standards, and internal/external contracts and some industrial best practices. Compliance risks may be assessed by Compliance Department, sometimes by Internal Audit Department or by some certification agencies/organizations as well such as ISO.

• *Internal audit risk assessment:* Risk assessments that are performed for Internal Audit purposes are to ensure that, operation level risks are thoroughly identified within the business processes and appropriate risk measures or controls are in place to prevent those risks (Clune, R., 2005).

• *Financial statement risk assessment*: This type of assessment is based on the information inputted by both internal and external parties of a company such as internal auditors, financial and business controllers, external auditors and daily operations. It is based on the risks that will arise from the material misstatement in the financial statements of the company, which may mislead the shareholders. This assessment is the based on financial reporting elements (e.g., materiality of the underlying accounts, transactions) and internal control effectiveness of the daily operations. (e.g., likelihood that a control may fail to operate as intended) (Carcello, J.V., 2005).

• *Fraud risk assessment:* This type of assessment intends to evaluate the potential of fraud incidents that may be incompliant with ethics and code of the organizations, and distract the daily practices and business objectives (Beasley, 1999).

• *Market risk assessment:* This type of risk assessment is based on external market risks and how they will affect the company's performance. It basically considers interest rate risk, currency risk, option risk, and commodity risk and performed by market risk specialists.

• *Credit risk assessment:* This type of risk assessment is performed against the risk that a borrower will fail to pay due to its agreement with the company. Evaluation includes not only the individual transactions but the whole borrower portfolio as well.

• *Customer risk assessment:* Similar to the credit risk assessment, it is for evaluation a customer's risk (and whole customer portfolio as well) that could harm the financial position and the reputation of the company. It is based on the evaluation of customer's creditworthiness, affiliations, and other relevant factors.

• *Supply chain risk assessment:* This type of assessment evaluates the risks beginning with logistics, to production of goods/products/services, supplier management.

• *Product risk assessment:* This type of assessment considers the risk attached with the company's product, its design, production, distribution, use by the customer and its disposal. It not only aims to understand the impact of cost but also the revenue, relationships with other products, relations with third parties etc...

• *Security risk assessment:* It is the evaluation of the possible weaknesses in a company's physical and logical security controls. Security assessment includes hardware components, operating system, applications, operations, and human factor.

• *Information technology risk assessment.* This type of assessment aims to understand and evaluate the risks that may be associated with organization's failure to catch up with the new technological developments required by the business or its system failures, of waste of technologic investments due to emerging new trends. This is one of the most critical risk factor for Telecommunication companies. As the technologies change rapidly (e.g. increase of 900 Mhz to 1800Mhz, 2G to 3G,), Telecommunication companies not only race with each other to serve it's customer with the best quality but race with the technology itself.

• *Project risk assessment**:*** This type of assessment is based on the risk associated with start-up, implementation and delivery of the projects. It is evaluates who are the stakeholders, when are the deadlines, and costs associated with the project.

The scope of risk assessment that management chooses to perform depends upon priorities and objectives that may change in time, slowly or rapidly again depending on the industry that the company operates in.

2.1.4 THE ROLE OF 'INTERNAL AUDIT' IN RISK MANAGEMENT

Before a company considers how to set-up risk management role, it is important to take a look at the role of other departments such as internal audit, internal control and finance. It is certain that the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes. Internal Auditors are involved in determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment of the following (Gramling, 2006):

- Organizational objectives support and align with the organization's mission;
- Significant risks are identified and assessed;
- Appropriate risk responses are selected that align risks with the organization's risk appetite; and
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.
- Risk management processes are monitored through ongoing management activities, separate evaluations, or both. Internal audit is an assurance process in nature; therefore, in order to maintain its independence, some of the ERM roles should be restricted for internal audit departments as presented in Figure 1 (Institute of Internal Auditors 2008) below:

Figure 1
Role of Internal Audit in Risk Management

Core Internal Audit Roles in ERM:
Giving Assurance on the risk management process Giving Assurance that risks are correctly evaluated Evaluating risk management process Evaluating the reporting of key risks Reviewing the management of key risks
Legitimate Internal Audit Roles:
Facilitating identification and evaluation of risks Coaching management in responding to risks Consolidated reporting on risks Maintaining and developing ERM framework Developing risk management strategy for Board approval
ERM Roles that should be restricted for Internal Audit:
Setting the risk appetite Imposing risk management processes Management assurance on risks Taking decision on risk responses Implementing risk responses on management's behalf Accountability for risk management

Source: Institute of Internal Auditors, "Role of Internal Auditor in Risk Management", Internal Auditor's Manual.

2.2 THE RECENT ISSUES ABOUT ENTEPRISE RISK MANAGEMENT

The Telecommunications industry is characterized by robust competition, vast infrastructure requirements, and very short turnaround times for identifying threats and assessing and mitigating their associated risks in order to minimize network downtime. Organizations in the telecom sector are constantly looking for methods and solutions to streamline their processes as a means of reducing organizational risk.

In addition, telecom firms must comply with regulations and requirements set by the local or global regulatory bodies or organizations. The investment necessary to meet these requirements can be significant, and telecom firms can realize substantial benefits by transitioning their risk and compliance efforts into a structured and controlled process. Therefore, implementation of an effective risk management framework will bring not only challenges but many opportunities together.

2.2.1. CHALLENGES & OPPORTUNITIES OF RISK MANAGEMENT IN TELECOMMUNICATION INDUSTRY

The importance of ERM is shifting at speed and the quality of a firm's ERM framework will become one of the factors which will impact the cost of capital.

Organizations that are able to manage risks within their risk appetite and provide reasonable assurance to their stakeholders regarding the achievement of the organization’s objectives will be the winners of the future. When the organization achieves these outcomes, management is better able to link growth, risk and returns, deploy resources more effectively, thereby reducing overall capital requirements and improving capital allocation, identify and take advantage of positive events quickly and efficiently, reduce operational surprises and losses. ERM helps management to recognize potential adverse events, assess risks and establish responses, thereby reducing surprises and related costs or

losses; helps to report with greater confidence Preparing internal and external information that is as reliable, timely and relevant; and finally satisfy legal and regulatory requirements.

2.2.2 CHALLENGES TO EFFECTIVE RISK MANAGEMENT

Every organization will have unique factors that must be addressed as part of the design and implementation of Enterprise Risk Management. An ERM survey that was performed by an audit company in 2007 showed that, most of the companies had troubles during and after the implementation of ERM systems and nobody's life was 100% easy. Table 7 (PricewaterhouseCoopers, 2007) presents the results that were obtained from 83% of large, U.S. based multinationals with 88% of their senior executives were interviewed. The most common challenges of ERM according to those senior executives were as shown below.

Table 3

Most Common ERM Challenges

Difficulty in quantifying risks	61%
Conflicting corporate priorities	60%
Difficulty identifying/measuring the potential benefits of ERM	60%
Timelines and quality of information	59%
Difficulty in imbedding risk management into different cultures and behaviors	53%
Availability of information	52%
Difficulty integrating risk management into business processes	51%
Lack of clarity, roles and responsibilities in managing risk	46%

Source: PricewaterhouseCoopers, Management Barometer ERM Survey, 2007.

Even though the process itself is tough, there are tips for a successful Enterprise Risk Management to keep in mind; obtaining senior management commitment and buy-in to the concept of enterprise risk management is important for its value to the business. Recognizing and accepting that Enterprise Risk Management is an ongoing process is a must and is not limited to episodic activities or initiatives. It is wise to avoid surprises, manage the change through the planning and execution of appropriate project initiatives which are appropriately controlled, managed and resourced.

ERM should be enhanced to maximize value, in addressing the concerns of all stakeholders: investors, senior management, board and regulators, who look for transparency, accountability, profitability and soundness. It should also provide a streamlined process, coordinated amongst groups, with a common risk vocabulary and classification. Risk monitoring should not be a 'tick-the-box 'exercise and risks should be monitored from both tactical and strategic perspectives.

Finally, one should keep in mind that organization's culture to support the development of more robust risk management processes and structure will not be ready for it in one night and change takes time.

2.2.3 TRENDS FOR THE FUTURE

The recent financial crisis in 2009 has exposed shortcomings in the risk management practices in not only in financial institutions but all industries, including Telecommunication as well. It is common that serious actions are taken in times when serious problems occur. Recent fraudulent accounting scandals resulted in regulators and companies be more alert and to take serious precautions. Especially regulators not only in abroad but in Turkey as well is considering additional oversight responses. Foreign acts or regulations can be summarized as; SOX 404 Act in USA for all NYSE quoted companies, Basel I and II for all financial institutions, Solvency II for all insurance companies. (Perrin,

2009). Local acts or regulations are as follows; SPK's "Corporate Governance Principles" for quoted companies, BDDK's regulation (5411/2/29-32) for all banking institutions, Sayıştay Internal Control and Risk Management Principles for all public organizations, Prime Ministry and Treasury Regulation (number 26913) for all insurance companies.

Besides regulators, credit rating companies such as Standard and Poor's, Moody's or Fitch Ratings Ltd had announced in 2005 that they will begin to assess the quality of ERM programs as an element in assigning credit ratings for all financial institutions. In 2008, that had made an expansion on the announcement and declared that they will use the ERM quality criteria not only for financial institutions but for all companies that seek credit rating as well starting from the second quarter of 2009. Even ISO had released "ISO 31000:2009" principles which generic guidelines on risk management. ISO 31000:2009 can be used by any public, private or community enterprise, association, group or individual. It is not specific to any industry or sector and not for certification purposes either.

Telecommunication industry is a very young industry in Turkey when compared to other industries such as banking or fast moving consumer goods. Risk management is new trend for those telecommunication companies; even some of them do not have a separate ERM department within their organization. Most of the existing risk management roles within these companies are occupied by transfers from internal audit, finance, or consultant positions. There are also cross-industry transfers from banks and insurance companies as financial institutions have at least FRM (Financial Risk Management) experience. Current risk management players believe existing efforts are not enough and they still need to work on it, but they see serious and solid advantage in implementing effective ERM systems.

Enterprise Risk Management is the rising star in executives' dictionary. It should be perceived as an evolutionary process, a process of continuous learning and adaptation to changes in our environment. ERM does not solely mean avoiding the downside; risks are also opportunities. If management tries to avoid all risk, the company will not catch the opportunities especially those that had recently emerged in the current Telecommunication

market. It is of course does not mean that management should be carefree in hunting new opportunities. Effective risk management is a process of making risk-based decisions, therefore maximizing the chances of success.

2.2.4. THE ORGANIZATIONAL OUTCOMES OF RISK MANAGEMENT

Organizational behavior has been a topic of management theory for several decades. Numerous frameworks for understanding organizational culture have been proposed, using a wide variety of ideas. Some focus on management's assumptions about employees, while others describe various patterns of behavior within entities. There have been discussions of the values espoused by an organization, the leadership styles of those in charge, and the type of language used within the organization. Regardless of the approach, the underlying thought is that organizational culture plays a critical role in key areas such as how major initiatives are implemented, how quickly the organization can react to market changes, and whether or not the organization can successfully navigate major changes in the business environment. Since ERM is a substantial initiative, and it is intended to help an organization be more resilient in times of uncertainty, it would not be unreasonable to expect an organization's internal culture to be a significant factor in ERM deployment. (Kimbrough, 2009) Indeed, ERM implementers are encountering challenges related to organizational culture. One study identified "organizational culture" and "organizational turf" among the top barriers to ERM implementation, encountered by approximately half of survey respondents (Miccolis, 2001). Risk Value Insights: Creating value through enterprise risk management - A practical approach for the insurance industry.: Tillinghast-TowersPerrin Monograph.) Another study found that about two- thirds of its participants were facing challenges in managing the cultural change required for implementing ERM within their organizations (The Conference Board, 2005).

A review of the literature provided insights into apparent links between ERM and the organic-mechanistic model. Descriptions of ERM suggest the desirability of certain cultural attributes. There should be a shift from the tradition of managing risk within

organizational silos to managing risks on a portfolio basis across the entire entity which leads to a requirement for effective communication and collaboration across the organization. Furthermore, ERM presumes that identification and communication of risks will occur freely and routinely, that is, there will be "risk transparency throughout an organization". These qualities appear to align with the organic characteristics of collaboration, lateral communication, and employee commitment to the organization's tasks. (Adrian R. Bowden, 2001). Meanwhile, definitions and frameworks describe ERM as a process that involves seemingly mechanistic qualities. It supports compliance with rigorous activities including regular risk identification, analysis, prioritization, monitoring, control activities, and the use of a common risk language. Adherence to such standards may be mandated from as high as the board of directors. These attributes lean toward the mechanistic end of the spectrum, which is characterized by insistence on obedience to superiors, employees needing detailed instructions, and a hierarchical chain of command (Mittelstaedt, 2005)

Some discussions of ERM have contrasted cultural attributes that appear to loosely parallel the organic-mechanistic model. Leech outlines a "Historical/ Traditional" approach and "The New Vision" for control and risk governance. (Tim Leech, 2000) The former includes management's role to assign duties and supervise staff, an environment driven by policies and rules, and limited employee participation. The "New Vision" has empowered employees, a culture of continuous improvement, and extensive participation throughout the organization. Similarly, James Lam contrasts two sides of risk management. The "hard side" includes risk oversight committees, policies and procedures, and audit processes, while the "soft side" involves risk awareness, people, trust and communication. While Leech strongly advocates the "new vision" for effective risk management across the organization, Lam supports a balance between the "soft" and "hard" sides. (Lam, James, 2003).

Both successes and failures in managing risk were reviewed in order to gain an understanding of the role played by organizational culture. Notable failures in risk

management have been blamed on cultural issues. The cultural factors identified as contributors to many implementation failures appear to represent both organic and mechanistic qualities. Organic characteristics supported for the prevention of implementation failures include:

* Innovation and collaboration when it comes to achieving the goals of the entity as a whole, and

* A network structure of communication, including laterally across organizational borders.

Mechanistic characteristics supported include:

* Vertical communication along hierarchical lines according to the organization's rules, and

* Clearly defined and specialized tasks, and the expectation that these tasks will be carried out precisely according to instruction.

By contrast, case studies of successful ERM implementations appear to lean towards organic cultural attributes. For example, they advocate "a culture receptive to change" and "a culture of continuous improvement" (Miccolis, 2001). In addition, frequent mention is made of the pervasiveness of risk awareness throughout the organization, as typified by the use of phrases like "managing risk is ingrained in the company's culture," "risk management remains a critical part of its culture," and "risk management is deeply rooted in the corporate culture" (Barton, 2002).

It is certain that board members, audit committees, Risk managers/officers should be empowered for fulfilling their risk management roles. As technology organizations such as Telecom companies face a complicated set of risks which should be well understood and fully addressed by all risk management related parties. This involves leading the way by institutionalizing systematic risk identification, assessment, and response initiatives, along

with the supervisory and cultural elements that will support ERM activities. Attention to these aspects of managing risk should help engineering managers not only to prepare for threats to the organization and its assets, but also to take risks more intelligently and productively.

2.3 MANAGING THE ENTERPRISE-WIDE RISKS IN TELECOMMUNICATION INDUSTRY

An effective risk assessment process is the preliminary requirement for effective enterprise risk management program as described in sections above. A linkage between risk assessment and risk management program should be well established to ensure that company is operating on a risk informed basis but also to ensure that risk based decision making is enable for all stakeholders.

Enterprise risk management enhances an organization's ability to effectively manage uncertainty. It is a comprehensive, systematic approach for helping all organizations, regardless of size or mission, to identify events and measure, prioritize and respond to the risks challenging its most critical objectives and related projects, initiatives and day-to-day operating practices. Enterprise risk management enables an organization to determine what level of risk it can or wants to accept as it seeks to build shareholder value. Managing risk more successfully may enable organizations to achieve their performance and profitability targets, prevent the loss of resources and ensure effective reporting and compliance. (The Committee of Sponsoring Organizations, 2004)

Enterprise risk management is not limited to one event or circumstance, it is a dynamic process that enrolls over time and penetrates every aspect of an organization's resources and operations. It involves people at every level and requires applying a portfolio view of risk across the entire organization. By embedding risk management techniques into day-to-day operations, an organization is better equipped to identify events affecting its goals and to manage risks in ways that are consistent with its risk appetite. Risk Management can be initiated internally as a result of an organization's targets and aims such as entering to new markets, new business development, maintaining or increasing operational efficiency. It can be mandated by regulatory bodies and industry related regulations such as "Bilgi Teknolojileri ve İletişim Kurumu" in Turkey for Telecommunication companies of Basel II for Banks, Solvency for Insurance industry.

2.3.1. PURPOSE AND APPLICABILITY OF ENTERPRISE RISK MANAGEMENT

For some organizations, the benefits of effective enterprise risk management are accepted as higher-level values e.g., the added capability to track similar risks across the organization. Other organizations seek more tangible benefits e.g., reducing or improving the allocation of risk management expenditure. Either way, management need to articulate the desired benefits of Enterprise Risk Management and the type of benefits realization processes required as part of the initiative. The Enterprise Risk Management Methodology can be used to help organizations develop a well-defined business case that clearly enforces management to ask "Why we need it and how we will use it", translates the objectives and potential benefits of Enterprise Risk Management, including specific areas requiring enhanced risk management capabilities. (Beecheer Carlson, 2010)

Organizations need the capability to put risks into a business context. This is best done by measuring risks in the same or congruent units of measures as business objectives. Many organizations have undertaken risk assessment processes without linking risks to corporate or business unit objectives. In such instances, the resulting assessment is likely to be a risk inventory grouped by similar risks with little context to what the organization is trying to achieve. In fact, the Enterprise Risk Management should ensure that risks are identified and assessed within the context of an organization's business objectives and goals and that the Enterprise Risk Management Framework is designed and implemented in support of these goals.

Management tries to balance the relationship between growth, risk and return. While there is often a tendency to focus on additional mechanisms for reducing risk, there may be opportunities to accept greater risks so long as the additional risk levels are understood and managed. When management is struggling to articulate and define their risk philosophy and risk appetite, the ERM approach can be used to help the board, audit

committee and management consider how its risk appetite and risks tolerance are determined, used and communicated. (Scarbrough 1998)

Many organizations have taken a “silo” approach to enterprise risk management - gathering and analyzing information based on the effect of risks to a single business unit or a single entity-level objective. ERM emphasizes the need to establish a portfolio view of risks - the understanding that a single risk can affect many objectives and that a single objective is affected by many risks. The identification and evaluation techniques used throughout the methodology can be used to help management create a portfolio view of risk and more efficiently integrate risk responses. (Tim Leech, 2009)

Organizations need the capability to assess the importance of risk to their objectives. Risk should be measured, either qualitatively or quantitatively, relative to specific performance measures associated with organizational objectives, whether financial, operational or otherwise, to be actionable. By using the same, or a congruent, unit of measure established for their objectives, the results are more meaningful to management and reduce the need for the development of separate measures. In doing so, Enterprise Risk Management becomes embedded into management processes. For some, management will accept ordinal measurement scales while others may desire interval or ratio measurement scales. ERM is flexible enough to be able to adapt to the measurement scale selected by management’s performance measurement program. ERM is not a one-size-fit all approach. It is easily tailored to meet unique organizational needs. It places appropriate emphasis on understanding the current organizational capabilities, working with management to develop the future vision and the plan to achieve this. The approach that has been developed is not linked to any one particular standard or framework but reflects the risk management principles that these standards define.(James Lam,2003)

Effective enterprise risk management requires appropriate and timely information that supports management decisions. An appropriate ERM methodology can be used to help an organization identify the information needed for enterprise risk management and to

help the organization implement appropriate information flows throughout the organization which gives additional consideration to the information and communication needs of the board, management and staff (Robert Philips, 2008).

2.3.2. KEY STAGES OF IMPLEMENTING ENTERPRISE RISK MANAGEMENT FRAMEWORK

The methodology that will be presented below consists of two stages; to assess and to design the enterprise risk management frameworks, based on the specific needs of a Telecommunication Company. Efforts for implementing these stages may vary from one company to another depending not only their time and capital investment but also the willingness to change.

First step is the "Assess", which is used to assess the current approaches to risk management and analyses the organization's enterprise risk profile. Next step "Design" is used for defining the future Enterprise Risk Management Framework and associated organizational business case (reason to implement an ERM system, expected outcomes for the business) and to design the supporting policy changes, processes, procedures, organizational changes, training and any supporting systems and technologies. This stage should include how to implement, monitor and continuously improve the policies, processes, technologies and organization developed to achieve the planned business outcomes and benefits from Enterprise Risk Management. (Ahmet Uğur Cebeci,2008)

Enterprise risk management initiatives may vary in scope significantly from one Telecommunications company to the other. Each implementation should be considered as a project and a project sponsor should be defined. Project sponsor may be one of the CXOs, Board of Directors or a Risk Committee of senior executives etc. It is important to determine the proper scope for each initiative before beginning projects or tailoring the methodology. Through out the project, management may need to make changes to the

scope but it must be carefully stated, the impact evaluated and the changes agreed with senior management before being implemented. The initial understanding of the project's scope may be refined during start up based on discussions with senior management. It is better to create a work plan for the completion of the Assess stage to determine the issues to be addressed and to define the boundaries of the risk management initiative. Scope should be revisited on an ongoing basis throughout the framework set up as it may change as more information is obtained about the organization and its strategic, operating and technological environments. Opportunities surfaced during the Assess stage may also change the scope of the remainder of the project but these changes should be formally approved. (Thomas Barton,2002)

2.3.2.1 ASSESSMENT STAGE

An enterprise risk management project may be undertaken for a number of different reasons and expectations of management including the following (Michel Crouhy, 2005):

- Need to broaden the view of risk management from being solely a business unit risk and control assessment activity;
- Lack of common understanding or awareness of risk throughout the organization;
- Lack of a common risk language and risk management competencies;
- Need to break out of continuous crisis management mode;
- Desire to protect corporate reputation;
- Board/regulator pressure to revise current reporting practices;

- Board/stakeholder pressure to understand the full range of risks facing the organization;

- Cost of risk is not currently understood or captured as a financial consideration;

- Risk communication is likely only after a loss or negative press to the organization; and

- Few risk management processes are defined and success depends on individual effort.

As the expectations of ERM implementation varies from one company to another, the scope of an enterprise risk management project will vary accordingly. Types of ERM projects may include:

- Performing an "Enterprise Risk Profile" for the organization;

- Assessing the current risk management capabilities of the organization;

- Preparing a business case for Enterprise Risk Management; or

- Implementing Enterprise Risk Management.

All of the different tasks necessary to formally begin the ERM framework setup should be completed at the beginning of framework set up. Risk of unplanned scope adjustments, significantly revised work products, misunderstandings and cost overruns can be eliminated with effective planning in Assess stage. ERM framework setup should be considered as one of the internal project of a company and no matter how small or unique, it will benefit from an appropriate degree of preliminary planning.

2.3.2.1.1.THE ANALYSIS OF ENTERPRISE RISK PROFILE

A risk profile is defined as a consolidated view of a set of risks which shows the impact and probability of each risk. Risk profiling can be performed at a number of different levels within a Telecom company e.g., across the entire organization, within specific business units and/or functions or for particular operating locations or countries.

The most critical factor for an accurate risk profiling is to understand the telecom industry itself, business objectives and associated critical success factors to be used as a basis in identifying risks. It is critical to;

- Identify the objectives, goals and strategies of the telecom business.
- Develop an understanding of the external business environment to provide

a basis for identifying areas where risk management is fundamental to the telecom business.

- Understand the competitive strategy of the business based on an understanding of its external business environment.
- Develop an understanding of the internal operations, using the value chain analysis, to provide a basis for understanding the business and identifying areas where risk management is required
- Identify strengths, weaknesses, opportunities and threats (SWOTs) of the business and their implications for risk management.
- Confirm the business “Critical Success Factors” (CSFs) based on a review of background documentation, industry research and interviews with senior management.

Different types of risk profile may be included in framework set up can be summarized as follows:

- An enterprise risk profile which provides a consolidated view of risk across the organization;

- High-level risk profiles of the inherent risks (inherent risks are those risks that the organization faces prior to any risk management activities);

- High-level risk profiles of the residual risks (residual risks are those risks that the organization faces once risk management actions have been taken); and/or

- Detailed risk profiles for specific business units, functions or risk types.

The objectives, scope, approach, responsibilities, timing and the format/content of the deliverables of a risk profiling may vary depending on different factors including:

- The project scope (if enterprise risk management is considered as an internal project of the company);

- The size and complexity of the organization;

- The current approach to risk management and existing corporate culture;

- Telecom industry dynamics in which the organization operates;

- The ERM project team's existing knowledge of the organization and its risk profile (the team may consist of Chief Risk Officer, Head of Finance, Internal Audit team, ERM or Financial Risk Management (FRM) consultants, IT specialists etc);

- Whether an enterprise risk profiling exercise has been conducted across the organization before -by departments individually- and the currency and quality of that exercise;

- Whether the former risk profiling exercise is going to be used as an input to develop an Enterprise Risk Management framework or whether the profile is to be used for other purposes (e.g., business planning, internal audit planning, submission to regulators); and

- The requirements and expectations of key project stakeholders (regulators, credit rating companies, business partners or shareholders)

The approach to enterprise risk profiling includes; identifying events and risks; identifying existing risk responses and measuring the risks. It is critical to validate the risk information that has been gathered and to determine areas that require additional analysis. The enterprise risk profiling plans should define the details of how these activities are to be performed, the objectives, scope and the outcomes (reports, risk matrices, risk heat maps, organization alternatives etc) to be produced. Once the events and responses have been identified, the exposures arising from these events are measured based on a initial consideration of inherent and/or residual exposure to produce an enterprise risk profile. Certain exposures may then be selected for more detailed assessment.

The enterprise risk profile is presented to board, risk committee or senior management (depending on the existing ERM function) together with any implications that the enterprise risk profile may have on the design of the organization's enterprise risk management framework and any "quick wins". Table 3 below represents the universe of enterprise wide high-level risk groups of a Telecommunication company which is the touch-stone of risk profiling. This high-level risk groups can be applied to most of the companies with a little bit tailoring according to their industrial and operational differences. It can be observed from the table that, risk do not always arise within the company itself but effected from the social, political, economic context as well.

Table 4
High Level Risk Types and Sub-Categories

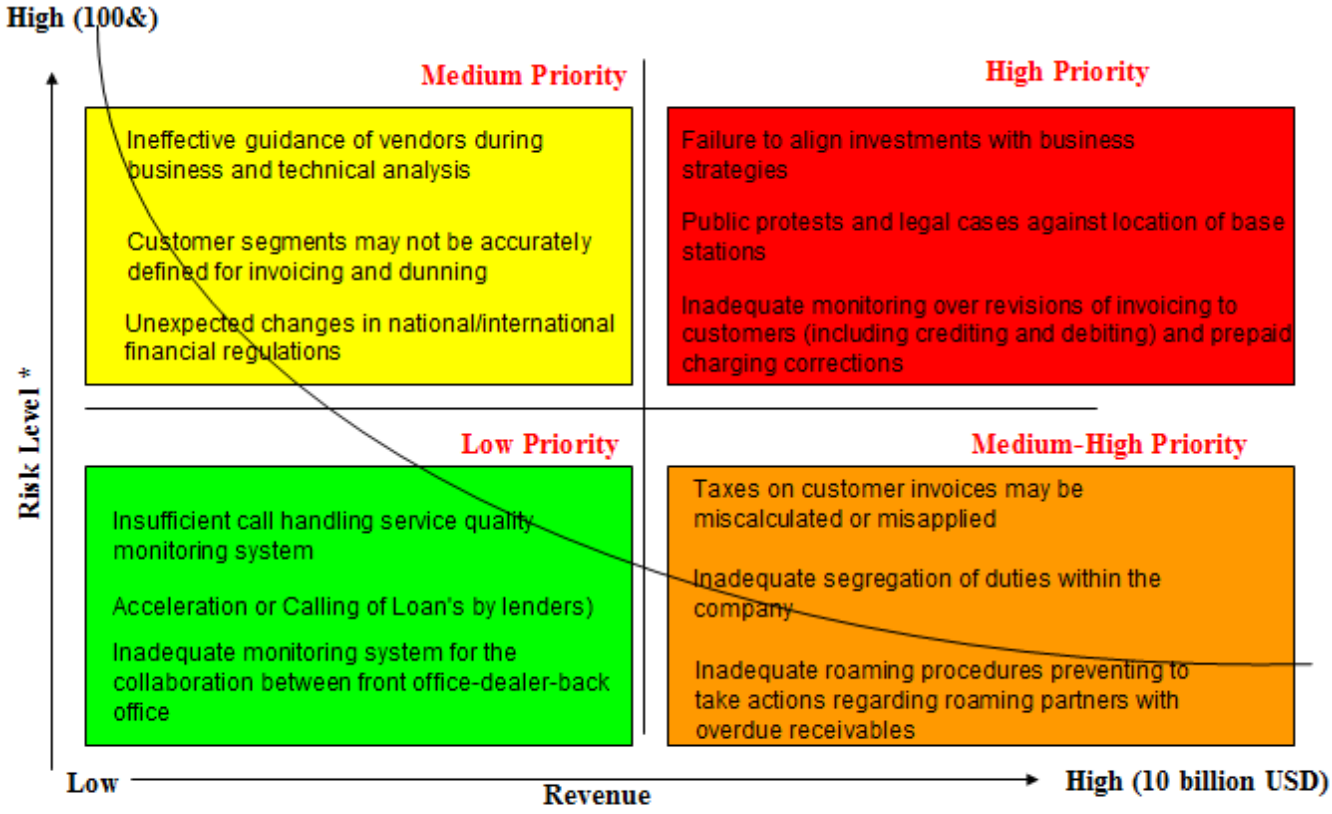
Risk Type	Examples		
Environment Risk			
	Competitor	Shareholder relations	Regulatory
	Customer wants	Capital	Industry
	Technological innovation	Sovereign/political	Financial markets
	Sensitivity	Legal	Catastrophic loss
Process Risk			
Operations	Customer satisfaction	Performance gap	Business interruption
	Human resources	Cycle time	Product/service failure
	Knowledge capital	Sourcing	Environmental
	Product development	Channel effectiveness	Health and safety
	Efficiency	Partnering	Trademark/brand erosion
	Capacity	Compliance	
Empowerment	Leadership	Outsourcing	Change readiness
	Authority/limit	Performance incentives	Communications
Information processing/ technology	Relevance	Access	Infrastructure
	Integrity	Availability	
Integrity	Management fraud	Illegal acts	Reputation
	Employee/third party fraud	Unauthorized use	
Financial	Price - interest rate, currency, equity, commodity, financial instrument	Liquidity - cash flow, opportunity cost, concentration	Credit - default, concentration, settlement, collateral
Information for decision making risk			
Process/ Operational	Product/service pricing	Contract commitment	Measurement (operations)
	Alignment		
Business reporting	Budget and planning	Financial reporting evaluation	Pension fund
	Accounting and information	Taxation	Investment evaluation
	Regulatory reporting		
Environment/strategic	Environmental scan	Valuation	Resource allocation
	Business model	Organization structure	Planning
	Business portfolio	Measurement (strategy)	Life cycle

Source: Deloitte and Touch, Risk Intelligence Manual, 2009

2.3.2.1.2 RISK MEASUREMENT TECHNIQUES

A number of risk measurement techniques can be applied to determine the extent of a risk. Measurement techniques may be quantitative, semi-quantitative or qualitative. For the purpose of enterprise risk profiling, qualitative techniques are generally used, whilst semi-quantitative and quantitative techniques may be used to examine specific risks in detail or to develop risk profiles for specific areas. Qualitative risk measurement provides a means of comparing the relative priority, importance or significance of risks and responses that have been identified which can then be used as a basis for assessing specific risks and responses in detail. (R Gregory, S Lichtenstein, 2006). Figure 2 below is a sample risk measurement graph for Telstra Corp. published by Standard and Poors on May 2009. It shows a detailed risk measurement with presentation of risk levels with different priorities and impact on the revenue.

Figure 2
Risk Measurement Graph for a Telecommunication Company :
Sample of Telstra Corporation



(*) Risk Level is calculated as a percentage where the maximum level is 100%
Revenue is displayed on a logarithm axis where the maximum is 10 Bln USD

Source: Standard and Poors, 2009

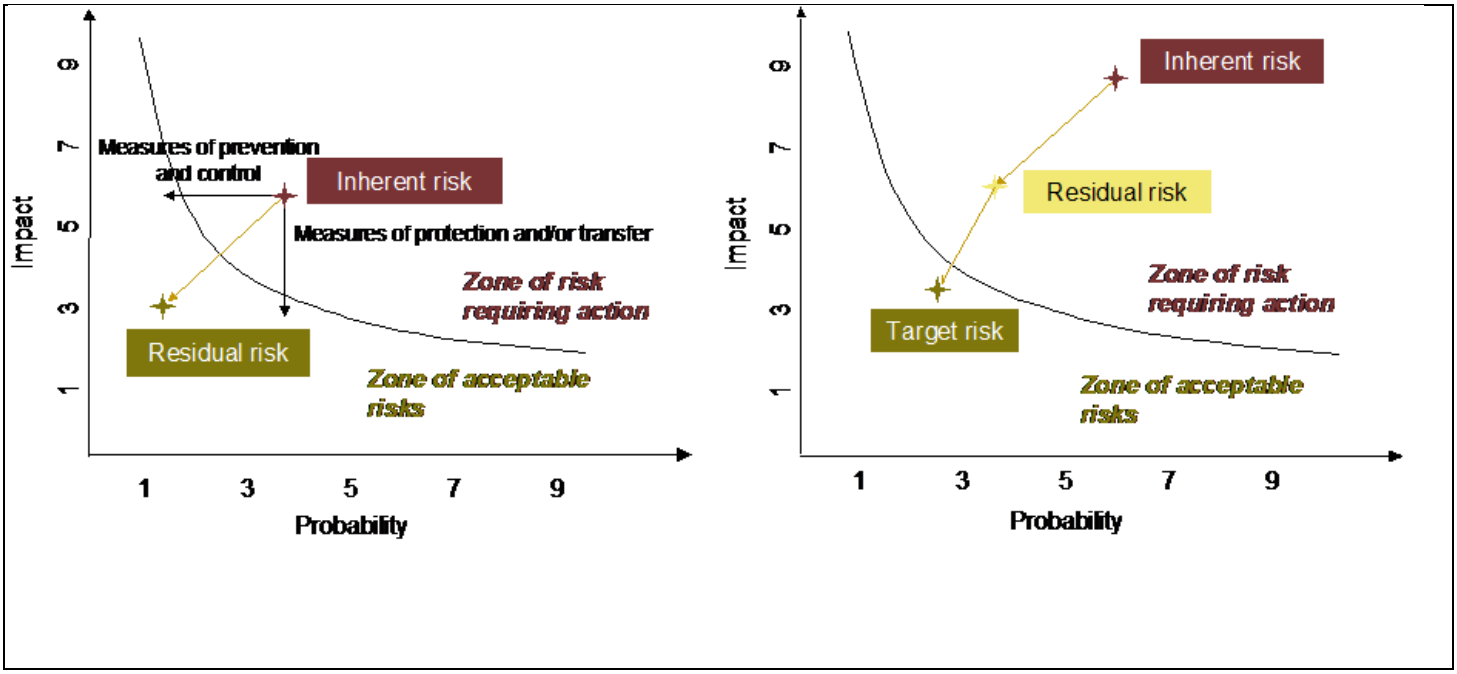
Qualitative risk measurement techniques include:

- Probability/impact scales and matrices;
- "Traffic light" or "heat-map" indicators for each risk where the color denotes significance, priority for management attention or scope for improvement; and
- Ranking of risks by description such as "most likely case, worst case and expected case" outcomes for each risk.

On the completion of a risk profiling exercise, the initial view of the inherent and/or residual risk exposures of each risk/portfolio of risks should be identified. Figure 3 below presents a sample scaling of inherent and residual risks according to their impact and probability. Determine whether it is appropriate or necessary to measure risks based on estimates of either their inherent or residual exposure or both where:

- Inherent risks are defined as those risks that the organization faces prior to any risk management activities; and
- Residual risks are defined as those risks that the organization faces once risk management actions have been taken (Bradly T. Borden, 2010).

Figure 3
Risk Scaling



Source: PricewaterhouseCoopers, 2004

It is critical to determine the approach to be used to identify events that may impact on the achievement of objectives where an event is defined as an incident or occurrence, from sources internal or external to a Telecom company, that could affect the implementation of strategy or achievement of objectives. Combination of event identification techniques in preparing an event inventory can be applied, such as (PricewaterhouseCoopers, 2004):

- Conducting desk research;
- Interviews with staff, management and relevant subject matter experts;
- Workshops with staff, management and relevant subject matter experts;

- Surveys and questionnaires;
- Reviewing internal data such as history of loss events, existing risk assessments, business plans and accounting records;
- Reviewing external data such as analyst reports and industry publications; and
- Reviewing documentation.

Figure 4 below is a part of a inherent risk matrix of a local telecom company. Ideally, for each of the events identified, ERM framework setup team should determine how the organization's existing responses to maximizing the potential opportunities and minimizing the risks for each event as well as for the portfolio of events is to be assessed. They should understand how the information obtained on event responses is to be documented and accumulated as well as any specific fields of information that should be collected for each response

Figure 4

Inherent Risk Assessment Scenario for a Telecommunication Company

Business Unit	Risk Description	I(A)	Availability Impact Rationale	I(R)	Reputation Impact Rationale	I(C)	Customer Impact Rationale	I(L)	Legal and Regulatory Impact Rationale	Process Related Mitigation Factors
Technology	Electromagnetic field levels (signal strengths/safety distance) of base stations may exceed regulatory standards	2	1	Single point interruption	3	Legislative potential investigations		5	may result pecuniary punishment to company by TA	Reactive actions may be taken against regulatory warnings All updates with respect to increase of safety distance are performed in line with regulatory requirements
Human Resources	Risk and process owners may not be clearly identified including those for cross-functional		Average availability impact due to unclear responsibilities	2	Minor reputation impact	2	Minor customer loss impact	3	Average legal and regulatory impact	High level processes and process owners are defined through following systems and methodologies such as; Assist+, Process governance
Finance	Failure to align investments with business strategies			2	Disputes among the group companies					Formally documented investment evaluation process including CFO, CXO approval is not available
Sales	Inability to reach potential corporate customer market share			4	Brand image for corporate sales negatively impacted	4	Potentially high quality customer cannot be acquired/retained			Policy and procedures are not fully supporting corporate customer sales

Source: Turkish Telecom, Risk Assessment Workshop,2009

An important part of the risk profiling plan is to determine how and by who the risk information obtained is to be validated so that it is accepted by key stakeholders as being an accurate and complete summary of the organization's risk profile. There are some approaches to be used to validate risk information such as:

- Using workshops with staff and management to develop, discuss, debate and agree on:

    1. a draft event inventory,
    2. the nature of responses in relation to the agreed event inventory,
    3. the ranking of risks and responses, and/or
    4. a draft of the risk profile;

- Obtaining sign-off on facts and interpretation of facts from relevant staff and management consulted throughout the course of the risk profiling exercise;

- Where differences in opinion exist over certain risks or responses, detailing these differences and the points of contention; and

- Engaging subject matter experts as part of the project team to assist in identification of risks and existing responses thereby adding credibility to the information gathering process.

2.3.2.1.3 RISK ANALYSIS TECHNIQUES

There are different types of risk analysis techniques that can be used during enterprise-wide risk analysis process. Usage of these techniques depends on not only the organizational structure and complexity of the business but also depends on corporate culture as well. Some of these techniques can be summarized as follows (Richard Clune, 2005);

Brainstorming techniques: By this technique, different types of creative group facilitation techniques that encourage participation from all group members regardless of their roles and relationships within the organization.

Scenario analysis: It is a systematic approach to considering and evaluating a series of possible future outcomes. By considering several likely scenarios, the analysis process is opened up to a much fuller range of possibilities, revealing insights previously overlooked when only one outcome is considered.

Focus groups :e.g., qualitative and quantitative assessment techniques.

Root cause analysis: e.g., Issue Definition Checklist, Multi-voting or Nominal Group Technique, Cause and Effect (Fishbone) Diagram, Force Field Analysis, Decision Matrix, Pareto Diagram. (Richard Clune 2005)

To assess current risk management-related systems and technologies; the organization's current use of systems and technology to support the risk management processes is determined. Systems that generate or make use of risk management-related information may include:

- ERP systems (SAP, Oracle and JDEdwards are the most common packages that are being used by Telecommunication companies);
- Functional or process-specific systems;
- Planning and reporting systems;
- Financial systems;
- Consolidation systems;
- Business intelligence systems; and/or

Depending upon the specific requirements of the ERM implementation, this task may be complex in nature and require the use of systems specialists as mentioned in scope definition and team setup in Assess stage.

In order to structure the design phase, a framework should be established for determining what to deliver in design phase. Here, I should note that, the most common framework which is used not only in telecom but all industries is the Committee of Sponsoring Organization's Enterprise Risk Management framework, which is also going to be explained in details at the beginning of the design phase within the following pages.

2.3.2.2. DESIGN AND IMPLEMENTATION STAGE

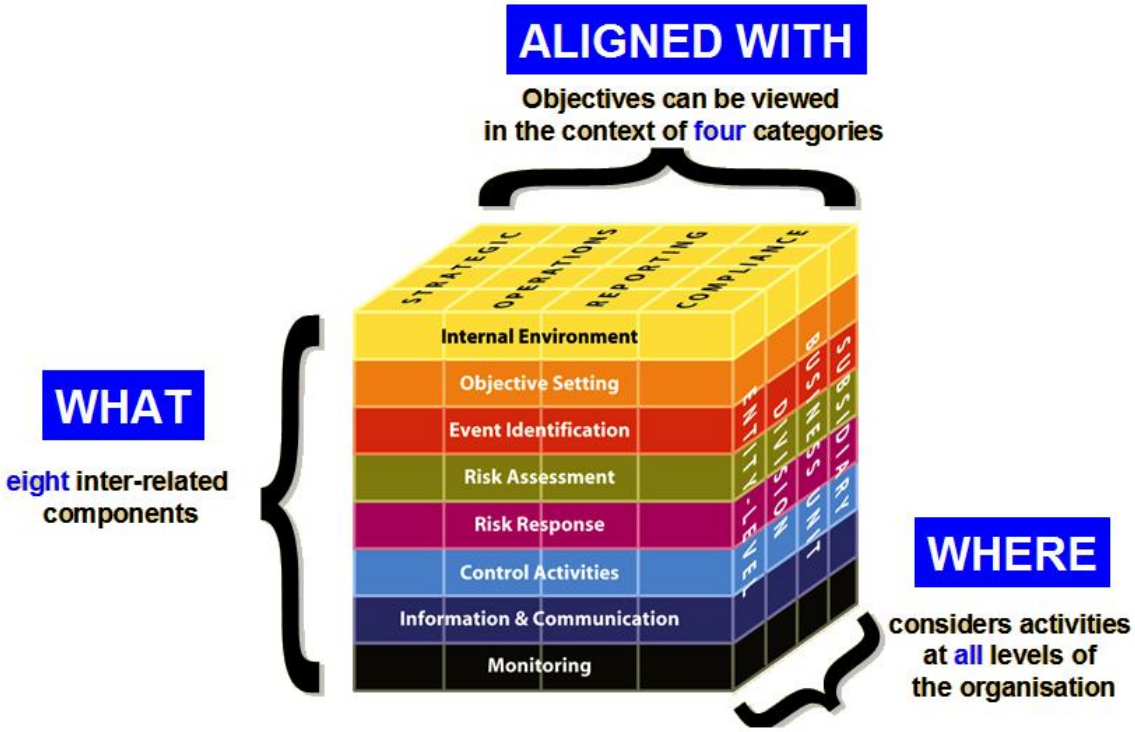
Committee of Sponsoring Organizations Enterprise Risk Management Framework had been used while defining development and implementation stages within the following pages. I have broke down the design and implementation stages to sub-phases; developing framework, implementation planning, conducting/starting the implementation activities, formulating risk response strategies, plans and policies. I have also explained briefly the tasks such as re-designing business processes that will effect from ERM implementation and organizational structure alternatives for ERM functions, which are post-implementation task and are additional acknowledgement for this thesis.

2.3.2.3 CONSTITUTION STAGE: COSO ERM FRAMEWORK

In 2001, COSO initiated a project to develop a framework that would be readily usable by managements to evaluate and improve their organizations' enterprise risk management. This Enterprise Risk Management – Integrated Framework expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management. While it is not intended to and does not replace the internal

control framework, but rather incorporates the internal control framework within it, companies may decide to look to this enterprise risk management framework both to satisfy their internal control needs and to move toward a fuller risk management process (Committee of Sponsoring Organizations, 2004). Committee of Sponsoring Organizations Enterprise Risk Management framework sets out the concepts that an organization should apply. It does not include guidance on how to implement the concepts in an organization. Below is the Figure 5 that displays the new Committee of Sponsoring Organizations Enterprise Risk Management Cube that has eight components and four categories. This Cube (Committee of Sponsoring Organizations, 2004) refers to all levels of the organization such as entity, division, business unit and subsidiary. Through out our development and implementation phases, Committee of Sponsoring Organizations Enterprise Risk Management framework will be referred as a basis for concepts to apply.

Figure 5
COSO ERM Cube with Eight Components and Four Categories



Source: Committee of Sponsoring Organizations, 2004

When a Telecom company begins to design stage, it should design the corner stones of the framework and ensure that framework implementation includes the following:

- A risk management strategy including risk appetite and risk tolerance;

- The definition of a common risk language to be used: Risk language changes from one industry to another, for example risk terms that are used in insurance and health industries are different from Telecommunication or mainly technology industry. Most companies, especially the ones with complex organizational structures and have high number of personnel may fail to define common risk languages. The definition of the risk management process to be used;

- Overview of the approach to be adopted to risk management-related policies. Such as if the company is going to create new policies or procedures or if existing policies will be revised to embed ERM related changes.;

- Determining how to integrate risk management into business processes and a list of the processes where this approach is to be applied. This bullet is crucial for all Telecommunication companies, as all of the business processes flow through complex IT systems and a large portfolio of applications are being used ;

- Performing an overview of risk management-related information flows including internal and external reporting requirements Most of the Telecommunication companies have a separate MIS – Management Information Systems Department or Unit that is responsible from data and report management, which is used by management for decision making. It is important to include MIS teams though the development to implementation stages of ERM;

- A target organizational structure with descriptions of risk management-related roles and responsibilities;

The framework strategy affects the implementation plan and may impact the overall cost of developing and implementing the Enterprise Risk Management Framework processes, technology and organization. There are many different standards and/or frameworks that a company may choose to use as a basis for implementation alternatives. A company, especially Telecommunication companies should select the most appropriate framework for their ERM implementation as Telecommunication industry is well governed and regulated. Companies should also take into consideration some additional requirements or legislations within their region (e.g. SOX, Solvency II etc). Selection of the standards and/or frameworks may be driven by corporate standards or rules, industry trends, regulations and country specific concerns. Most common publicly available standards/frameworks are such as (A.Scott, 2004):

- COSO Enterprise Risk Management Framework;
- Generally Accepted Risk Principles (GARP);
- Basel II - the New Accord to be issued by the Basel Committee on Banking Supervision; and
- AS/NZS 4360:1999 Risk Management, the Australian standard on risk management.

There are constraints and drivers for Telecommunication Companies while generating risk management frameworks. These constraints and drivers are identified through the "Stage I: Assess" which we have to deal or sort it out in "Stage II: Design and Implement" as well. Some of them are as follows (Ahmet Uğur Cebeci 2008);

- Existing risk culture;
- Existing risk languages;
- Existing risk management policies;
- Enterprise risk profile;
- Enterprise risk appetite;
- Existing risk management functions;
- Extent to which a consideration of risk is embedded into organisational policies and business processes.
- Existing organisation culture (whether the company is a local company, multinational company or recently acquired group company etc);

- Existing organisational structures (All of the players in Turkish market are sized as 500 to 1500 employees with complex organizational structures and different types of organizational hierarchy);

- Business objectives and strategies;

- Relative sophistication of the organisation's systems and technologies; and

- Change readiness of the organisation and the level of senior management support for the changes required by the implementation of an ERM framework.

Management should ensure that constraints do not become barriers effective risk management framework setup. The drivers/constraints can be used as an input to costs and benefits analysis for ERM implementation.

There are some techniques that can be used for designing the most appropriate ERM framework for a company. Brainstorming and Critical Success Factors (CSF) are the techniques that can be used for a Telecommunication company. Brainstorming technique is a creative group facilitation technique that encourages participation from all group members regardless of their roles and relationships within the organization. The emphasis during brainstorming sessions should be on creativity and idea generation and a non-judgmental atmosphere is essential. CSF is a technique that can be used to analyze and prioritize a set of alternatives by determining the extent to which each alternative supports the achievement of the organization's CSFs. CSFs are those few activities that must be executed well for a business process to be judged successful (Robert R Moeller, 2007)

2.3.2.3.1. IMPLEMENTATION PREPARATION

Implementation of an ERM framework consists of some steps which may change from one industry to another. For Telecom industry, there are some required steps to be

taken for an effective implementation. Steps can be summarized as (Ahmet Uğur Cebeci, Işılda Arslan, 2008);

I- Finalization of the implementation ERM strategy: The required level of ERM's centralization. The level of centralization may vary depending on the nature of the risks. For example, it may be important to centralize the management of the risks associated with variations in foreign exchange rates. This may require that a policy is developed at an enterprise level and cascaded down to all business units or subsidiaries. Alternatively, an Environmental Heath and Safety policy may be more appropriately developed at business unit or subsidiary level based on a few good practices defined at an enterprise level through working sessions with representatives of the business units or subsidiaries. Another point to consider is to determine the required level of integration of risk management with business processes.

II-Setting up the ERM organization: Organizational structure, designing roles, responsibilities and ownership alternatives. Point to be included may be;

- Changing the roles of senior management, the board and the Audit Committee;
- The need for a Chief Risk Officer and the associated reporting lines;
- Role of Internal Audit function;
- Changing existing job descriptions and roles; or
- The need to establish a risk and governance committee.

III - Determination of the required risk management information flows and associated information outputs : Table 4 shows a set of information needs for a Telecommunication Company, which is displayed by audience and frequency that may need to be generated by the information flows. Taking into consideration that some of the positions/audience presented below may not be applicable for all companies, some of the

information needs can be combined at one audience according to the organizational size and structure of the Telecommunication Company. (Colquitt, 1999)

Table 5
Information Needs of a Telecommunication Company by Audience and Frequency

Audience	Information Needs	Frequency
Operational Manager	• Review the list of risks owned around each sub-process and current status (i.e., most recent assessment) of each risk. • Review the list of controls owned around each risk and the control effectiveness. • Review the list of outstanding signoffs due for each risk and each control. • Review the list of new risks and controls. • Review remedial action progress.	Monthly Monthly Weekly Weekly Monthly
Senior Manager	• Review risk profile and list of risks around a process. • Review the performance of the related controls. • Review remedial action progress. • Review the list of outstanding signoffs due for each risk and each control. • Review the list of new risks and controls.	Monthly Monthly Monthly Weekly Weekly

Audience	Information Needs	Frequency
Business Unit Leader	• Review the business unit risk profile and supporting details • Review new risks raised and discuss potential mitigating controls • Review the extent of business unit control performance • Review and approve business unit progress on resolving control issues.	Monthly
Risk Manager	• Prepare reporting summaries for business unit leaders. • Prepare reporting summaries for Risk Management Committee. • Review consistency of content captured by the business units. • Analyze trends in risk profile and levels of risk exposure and control effectiveness. • Review issues and actions that have been raised. • Review and update business unit data structures.	Quarterly Quarterly Monthly Quarterly Weekly Quarterly
Risk Management Committee	• Discuss the risk profile of the organization. • Review particular concentrations of risks along with the underlying risk details. • Discuss overall control performance. • Decide actions for key issues. • Identify critical issues for Board attention.	All Quarterly
Board	• Decide actions for critical control gaps. • Decide actions for critical risks.	All Quarterly

Audience	Information Needs	Frequency
Internal Audit/Legal and Compliance	• Review list of high exposure business units. • Review exceptions in list of risk and control signoffs that may indicate control weaknesses or ownership incompatibilities. • Review samples of risk assessments for consistency of risk framework application. • Review lists of controls. • Review remedial action progress and status of all issues rose.	All Monthly
Regulator	• Review list of exposures across all business units. • Review list of controls.	Periodic

Source: Colquitt, "Integrated risk management and the role of the risk manager". Risk Management and Telecom Review,1999.

IV- Determination of the systems and technologies needed to support the information flows and organisation. Various alternatives may include changing existing systems to incorporate new or amended risk management-related processes; or acquiring new systems to support new or amended risks management-related processes.

Where the adoption of a new system is key to the implementation of the risk management framework alternative, it may be necessary at this time to complete a high level review of different solutions to determine the availability of process execution alternatives and the degree of fit. Depending upon the particular circumstance, this high-level review may determine whether, for example, a package software solution is available to meet the organization's requirements or whether a custom software solution or a package software

solution supplemented with custom code will be required. Some of the following activities may need to be completed as part of this process:

- Preparation of a high level requirements specification;
- Identification of potential suppliers;
- Production of a Request for Information (RFI); and
- Completion of preliminary evaluations of RFI responses.

V – Determination and monitoring of performance measures for ERM implementation. Performance measures vary according to the specific requirements of the organisation but may include for a performance over a specified timeframe such measures as:

- Percentage of employees who have successfully completed risk management training;
- Having less than five environmental incidents per year; and/or
- Achieving earnings volatility due to foreign exchange of less than 10% over a one year period.

VI – ERM training and change management (Vicky Arnold, 2009): Training requirements should be defined for transitional needs and ongoing implementation of the Enterprise Risk Management Framework). Training needs should be assessed during the implementation and training courses can be designed and delivered to change or improve existing skills of employees or at least increase the awareness and to communicate the requirements of the organisation's risk management goals to them.

Implementation plan for ERM framework should clearly define the planned business outcomes, cost of the implementation and need for a maintenance, it's measurable

benefits, responsibilities for achievement of those business outcomes and benefits, barriers for implementation, required time frame and risks that will arise with the implementation (as implementation of an ERM framework will effect the whole business processes even the systems within the company)

During the design and implementation phase, it is important to receive risk responses from senior management or Board of directors and document risk management alternatives to each identified risks. Taking into consideration that risk response development takes time, management may decide to review the risks with high or medium-high priority. Conducting workshops is a good method to define risk responses and how these responses will be taken to live. It is also important to define who will be the audience of the workshop as deciding how to manage risks, whether to mitigate, avoid or transfer requires a level of high seniority and authority in decision making.

Design and implementation workshops should consider such items as the extent to which the alternative supports achievement of the organization's planned performance levels, planned business outcomes, benefits and benefits measures, performance targets that are to be set for each alternative, timeframe for implementation, actions that need to be undertaken to address each alternative, the cost/benefit calculation that has been prepared for each alternative, the implementation issues, barriers and enablers for each alternative, the risks associated with each alternative and finally the classification of quick wins and opportunities which may constitute separate projects for the long run.

It is important to discuss all components of each alternative that have been defined to address the policies, procedures, processes, organization and technology that are required. Approval and confirmation of the project sponsor or board is crucial. The workshop may identify changes and revisions that need to be made to the selected different risk management alternatives.

2.3.2.3.2. CONDUCTING IMPLEMENTATION ACTIVITES

The implementation of the Enterprise Risk Management Framework may be a large, multi-year effort for organization-wide initiatives or staged implementations. An incremental strategy (multi-phased) may reduce some of the inherent risks associated with a large project implementation effort and provides a greater capability to be more responsive to changes in the business environment during the migration and implementation periods. Especially in complex environments such as Telecommunication Companies, implementation periods are in comparatively long terms, and require the involvement of multi teams, not only senior management but also operational level departments as well. Involvement of Internal Audit and IT Department is crucial as implementation touches core control points and core applications that reside on the main business processes and systems that are used by those processes.

Incremental implementation approach supports the ongoing use of current processes and technologies including enhancements to support business changes that cannot wait for the full implementation of the Enterprise Risk Management Framework. It also reduces risk of failure by completing migration and implementation in more manageable pieces. It helps building workforce competencies in manageable increments and is useful in delivery of interim benefits quickly while working towards the end target state. With an incremental implementation approach, the current risk management processes, technology and/or organization structure may need to continue to operate in parallel with the planned enterprise risk management framework for a period of time. Also, there may be a significant impact on resources during the parallel operation of the old and the new. (Walker, 2002).

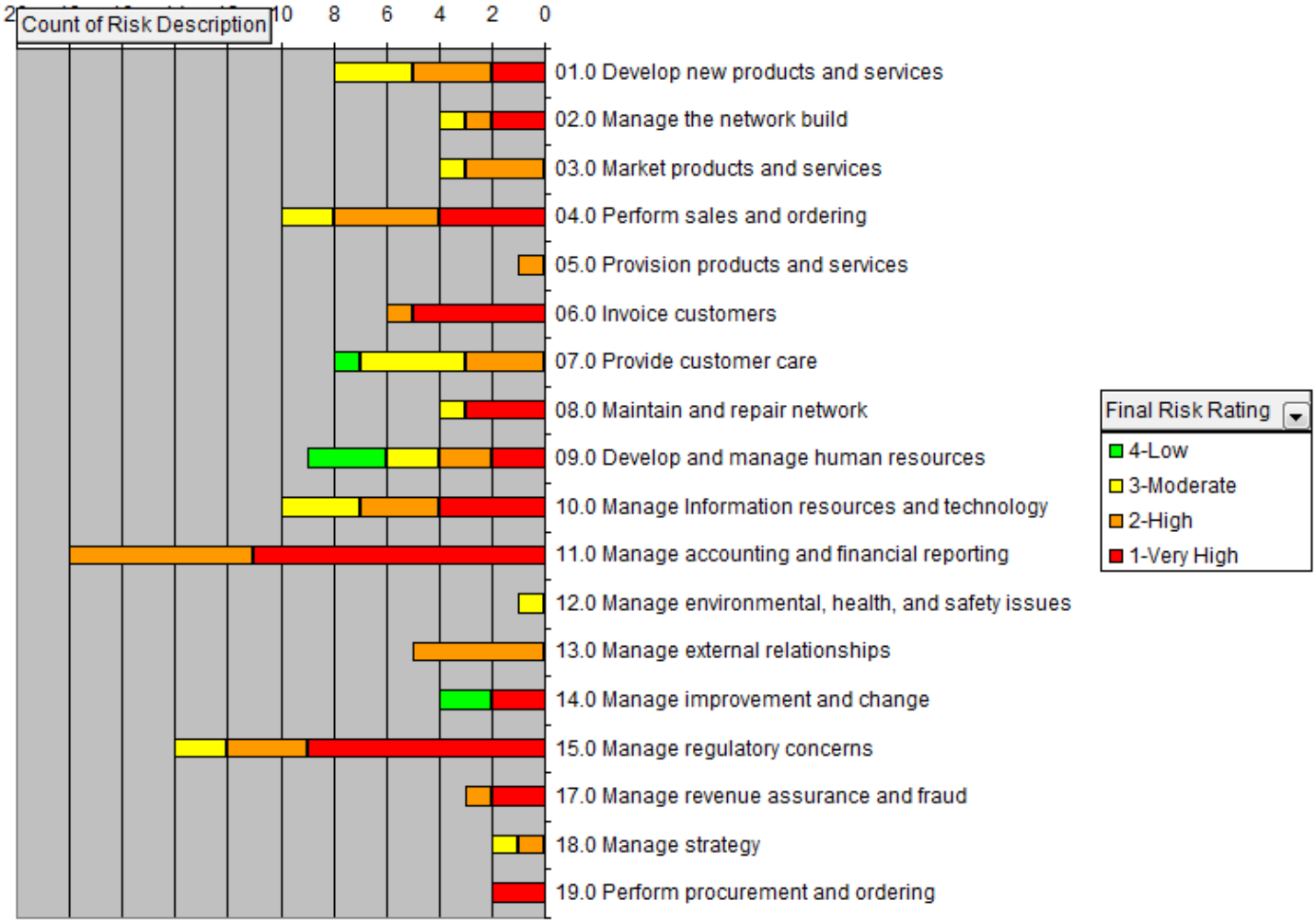
When a phased implementation approach is considered, the need for and cost of re-working the earlier phases to integrate into the later phases must also be determined and measured. A direct implementation approach may be simpler since all of the implementation activities are performed as continuous sequence of events. However, this

approach may be risky for Telecommunication Companies because of the large scale of activities required in a compressed timeframe and some critical service systems may be down for a while, which cannot be tolerated.

2.3.2.3.3. FORMULATING EFFECTIVE RISK RESPONSE STRATEGIES AND PLANS

Appropriate risk responses are determined after a risk assessment performed before design phase, to mitigate risk to an acceptable level within reasonable costs. Figure 6 is a risk rating of a local Telecom company. It lists the major risks that were identified after a risk assessment performed on the existing daily business operations. It is observed from the figure that, risk assessment was performed on 19 major areas of operations including regulatory compliance, revenue assurance, sales, marketing, business development and after sales etc. which are displayed on the right column. Number of risk that were identified though the assessment and was scaled at the top, from 0 to 20. The colorful bars that align horizontally represent the risk identified for each business area and the colors indicate the severity of the risks identified. It is possible to observe that business areas such as “Accounting and Financial Reporting”, “Regulatory Compliance”, “Sales” and “Information Technology” are the top four risks with severity of moderate to very-high. The figure should be used by management to determine where the most critical risks are accumulated and what is the urgency to create action plans to manage those risks.

Figure 6
Risk Rating for a Telecommunication Company to be used in Implementation Plans

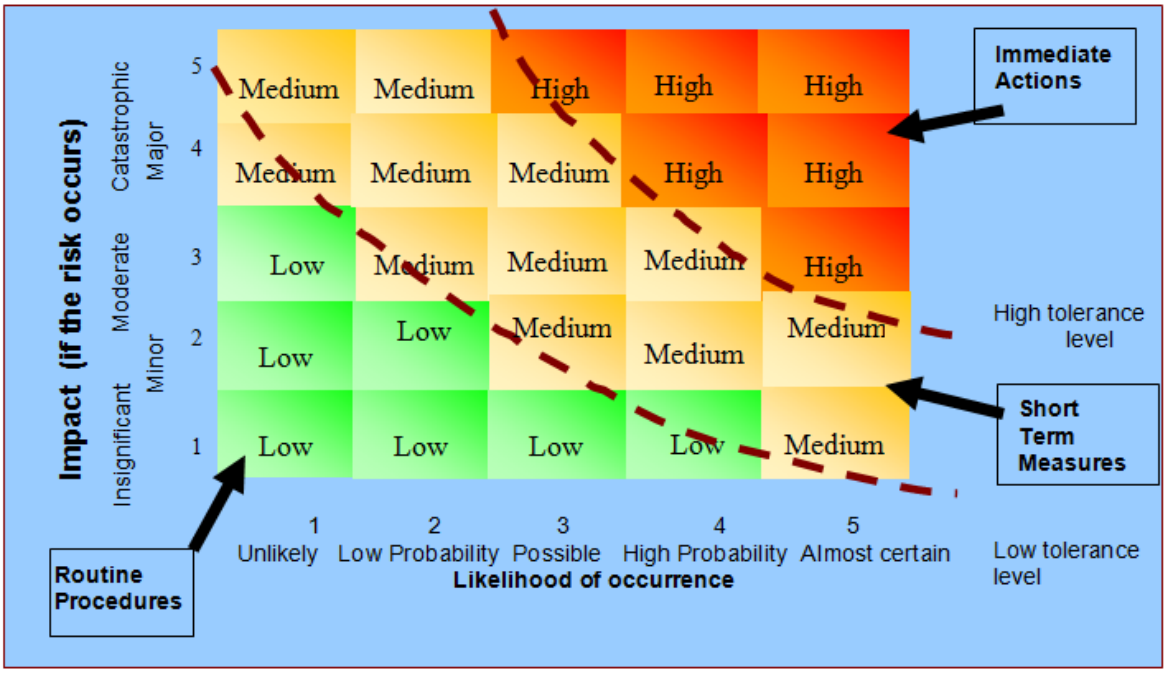


Source: Turkish Telecom, Risk Assessment Workshop

A Telecommunication Company's inherent and residual risk profile presented on the Figure 7 below, these risks are monitored against the target risk profile. As it is possible to determine from the figure, some of the risks are estimated to have a high impact and high probability to occur, therefore some of them need immediate actions to be taken. E.g. Risks that are related with "Number Portability" and related "Customer Loss" or "Inability to Comply with 3G technology" can be counted as risks with high impact and high likelihood

that many of the players in local market is facing. Therefore such risks are in the "Immediate Action Plan" of Telecommunication senior managers. This type of assessment should be used for prioritization of actions taken to manage those risks. If we were to place those risks within the table below, they would reside between short term measures and immediate action curves.

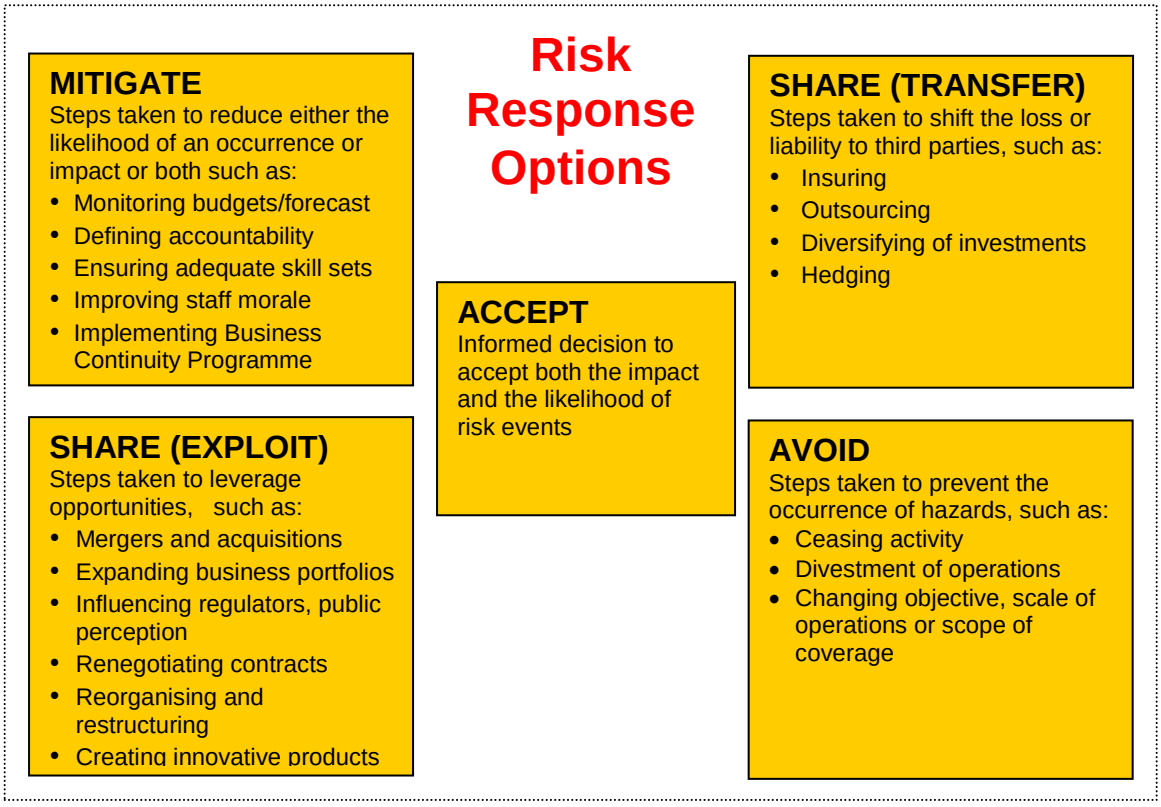
Figure 7
Risk Map for a Telecommunication Company



Source: Turkish Telecom, Risk Assessment Workshop

Risks can be dealt with in various ways. The risk response options include all possible management response to risk, whether viewed as opportunities, uncertainties or hazards. It should be kept in mind that, risk responses are selected by senior management and board of directors according to a company's mission and strategy. Issues such as financial position, market regulation, competition etc effects the risk appetite and risk tolerance limits of the management, therefore effect the decision to select appropriate risk options. The risk response options and examples of activities under each option are outlined in Figure 8 below (Michael Muehlen, 2005):

Figure 8
Risk Response Options for Planning Implementation Strategies



Source: Michael Muehlen, Danny Ting Yi Ho, "Risk Management in the Business Process Management Lifecycle", 2005.

Regardless of what a company chooses as a response option, senior management and risk management department should at least ensure that all risks are evaluated and are given a response. Telecommunication is a comparatively young industry in Turkey and some of the risks were being identified even at the last moment they occur. Also the business processes and systems are very complex, therefore management may seek the involvement of internal and external specialists/consultants for evaluation of risks and determination of risk responses. Table 5 below list a bunch of sample Telecommunication risks that were identified during a risk assessment workshop for a local Telecommunication Company in Turkey, it is possible to observe the risk category, the risk definition itself together with the actions to be taken to mitigate the risk.

Table 6
Risk Response Alternative for a Sample of Telecommunication Risks

Risk Category	Risk	Response
Competitive Environment and Macro-economic environment	Competition on price and subscribers as well as general economic developments may result in losses of revenues and margins. This may have an (adverse) impact on the valuation of assets In addition, competition is driving complexity in offerings (such as bundled arrangements). Revenue recognition is becoming more complex and not meeting targets may drive more aggressive revenue recognition. Inappropriate revenue recognition in general and in particular in the areas of	Review of the company's triggering events analyses and impairment tests; Use of specialists (CFR) to validate input data and valuation models; Increased focus on the accuracy of revenue recognition in compliance with applicable reporting standard e.g. IFRS. Procedures include review of significant contracts and product offerings on appropriateness of revenue recognition, mainly focused on accounting for multiple element arrangements and

	multiple element arrangements and gross versus net reporting issues are also risky.	gross/net reporting issues. Where possible, the company's internal procedures in this regard are tested.
Regulatory Environment	Given the highly regulated business, compliance with regulations is essential for a Telecommunication company and requires specific attention in our audit. Not only because of the financial impact (penalties if regulation is violated, revenue recognition if tariffs are not appropriate), but also because of the reputation impact.	Extensive procedures to ensure compliance with applicable laws and regulation, such as: Testing of internal controls that ensure compliance with laws and regulation such as internal review and authorization of contracts, input of prices and the 'softer' COSO components; Review of regulator's website and other communication to identify relevant regulatory developments and status of pending discussions; Review of significant contracts and pricing/discount schemes on compliance with regulations; Review of internal documentation of claims and litigation and discussion with responsible managers/officers of the nature and impact of these matters.
Supply Chain	Telecommunication operators are highly dependent on the reliable and continuous operation of their supply chain which includes the technical infrastructure and the IT systems. Disruptions in the	Extensive use of IT specialists in testing IT general controls and application controls. Testing of input-output controls as far as control is (can be) executed by the

	infrastructure and IT systems are a risky. Where key activities are outsourced, the company may not have sufficient control over these activities and reliability of the information may be hampered.	operator. Use of a SAS 70 report if deemed necessary.
Environmental, Social & Ethical	Most Telecommunication operators are concerned with the impact of legal claims, reduced usage and new regulation as a result of the potential health risks resulting from wireless communication. Not only could the outcome of claims have a significant impact also could new legal or constructive obligations arise which could impact the valuation of assets or recognition of provisions (Provisions for environmental liabilities/ potential Asset Retirement Obligations).	Review of (developments in) legal requirements and the company's external communications (for example environmental report) to identify the company's legal and constructive obligations.

Source: Turkish Telecom Risk Assessment Workshop,2009

2.3.2.3.4. FORMULATING EFFECTIVE RISK MANAGEMENT POLICIES

Defining a clear set of risk management-related policies provides a statement of an organization's perspective and approach to the management of risk. Policies provide a baseline statement around which the organization's risk management processes and procedures can be developed. For example, the organization may have requirements for separate policies that address:

- Legal requirements of a specific country, e.g. Turkcell and Vodafone uses policies for compliance with SOX 404, as the company is quoted in New York Stock Exchange ;

- Specific industry regulations e.g. Telekominikasyon Kurumu, 406 Telgraf ve Telefon Kanunu;

- Business activities of a particular business segment; or

- Specific business activities.

The risk management policies should be integrated as part of the organization's existing governance structures, policy setting and communication practices. They should reflect the organization's risk management perspective and risk management practices i.e., the organization's risk appetite and tolerances. They need to express the organization's objectives in relation to the management of risk; and should meet the mandatory requirements for risk management.

2.3.2.3.5. DESIGN PROCESSES AND PROCEDURES FOR ERM IMPLEMENTATION

The design of processes, organization roles and responsibilities and supporting systems and technologies is interrelated and phased tasks in nature. Design decisions made in any one of these areas, impacts the others especially for the Telecommunication companies that staff size is huge, processes are complex and inter-related and systems are high-tech and complex. For this reason, the tasks in this phase should be conducted in parallel with design of ERM roles and responsibilities and ERM related systems and technologies. Process design may be undertaken at a number of different levels of the organization including (Rolf Olsson, International Journal of Project Management "Is The Risk Management Process Enough?",2007, pg 745-752):

- At an enterprise-level - designing enterprise-level processes that define how risk management is to be integrated across the business;

- Across support processes at a business unit/function level - designing specific risk management processes e.g., credit risk assessment process; and

- Across primary processes at a business unit/functional level - embedding risk management into selected business processes e.g., embedding risk management into strategic planning or budget planning processes.

Most process design activities should focus on incorporating risk management into existing business processes. New processes may be required to address enterprise-level information and communication-related processes where new reporting requirements are envisaged and for specific risk management support activities. Once the process designs have been prepared, the design layout for the procedures that define how the process tasks and steps are to be completed should be prepared.

Before starting any process mapping or process analysis, it is important to;

- Establish the purpose of the process maps - There are many reasons for the process maps being prepared and the intended purpose must be clearly stated and agreed internally within the company.

- Confirm the audience(s) for the process maps is important as the audience(s) for the process maps may be many and varied, the different audiences may require varied amounts of detail or related process information and data;

- Standards should be determined for content Maps should be consistent in both look and feel as well as having consistency of content. This assists not only readability but when maps are prepared for different areas of an organization; they can easily fit together or be grouped. The use of a common tool may affect the standards

definitions and this aspect should be considered in conjunction with the recording approaches to be used to gather data and to store the maps;

- Level of detail required should be determined at the beginning - There are many possible levels of detail at which data can be gathered relating to different elements of a business process. Careful early consideration of the purpose and usage of the maps can clarify what information and related level of detail is required and which can reduce the amount of unnecessary collection effort and analysis (Generally accepted business process flow techniques are from Level 0 to Level 5). A wide range of tools exist for mapping and recording processes as well as using manual recording. The selection and usage of the most appropriate toolset should be determined before work commences. It is observed that the most common tool that are used for drawing process maps is MS Office Visio; and

- Scope should be confirmed for each process - Apart from process scope, the limits or boundaries of each process must be defined initially as there are many alternative definitions of boundaries e.g., should all interfaces or linkages to other systems be included or not. It may also be necessary to state which items are specifically excluded from analysis or consideration;

- Determining the information gathering approaches to be used is crucial - Different information gathering approaches are suitable for specific situations and it is important that the alternatives are matched appropriately before work commences. How much supporting detail (e.g., cost, duration, queue times, ownerships, and responsibilities) needs to be collected for various tasks together with its means of storage needs to be specified to avoid collecting redundant information.

When designing new processes or changing existing processes, the work steps will vary depending upon the scope of ERM implementation (Ahmet Uğur Cebeci, 2008):

- Redesigning existing processes - this is where existing processes are revisited to improve performance or to incorporate the risk management components. This may also include ceasing parts of processes;

- Reworking the way a process is executed - here the process tasks and steps may remain largely the same but how and where the process is executed may be changed (e.g., transfer to a Shared Service Centre);

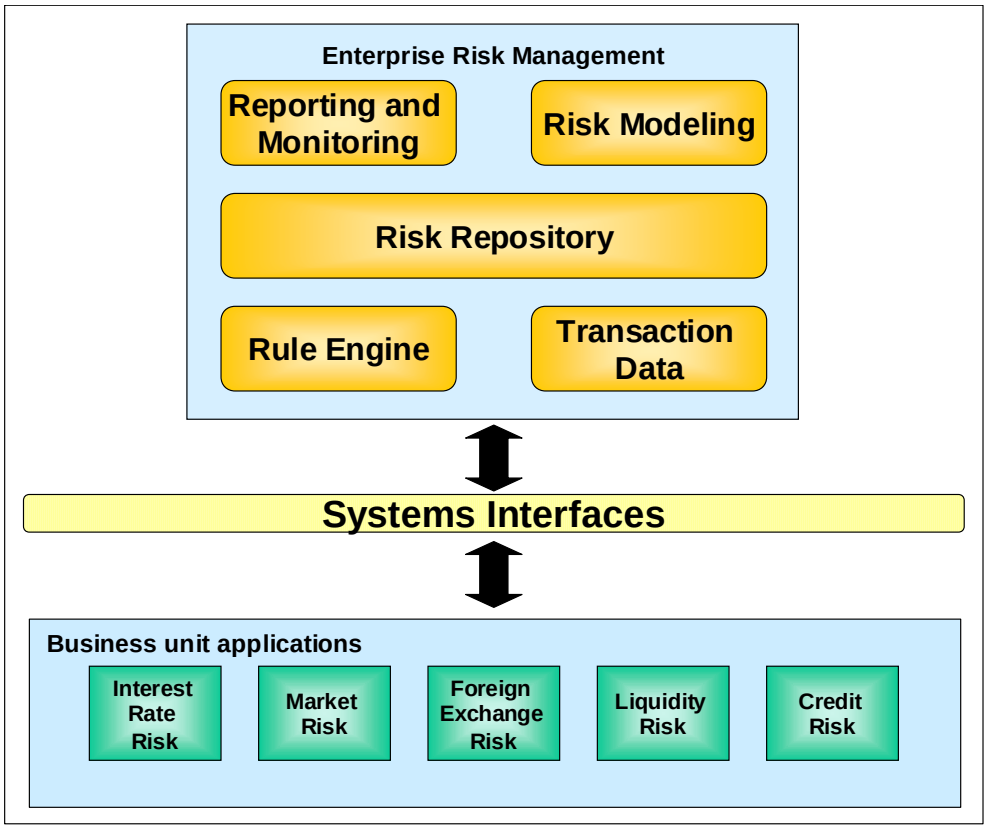
- Replacing the process - here the focus may just be upon gathering existing performance measures, considering migration issues and capturing experience to avoid problems being replicated in the replacement process;

- Removing the process - if a process is to be removed or replaced, the focus may be on the overall process performance measures to show the impact of the removal and the boundaries or connections to other processes which have to be changed; or

- Outsourcing the process - here the process may need to be at a lower level of detail to ensure that all nuances of the current process are captured.

The IT systems and application portfolio of the Telecommunication companies are extremely complex for Telecommunication Companies. It is the management's decision to use a tool or a system for risk management. The company may either choose to develop systems and applications via using its internal resources or may choose to buy and implement a off-the shelf package to adapt to its existing infrastructure. In either way, it is recommended for an ERM system to have a capacity to store transaction data and risk repository (events, incidents, risk, responses, controls, criteria's etc) regarding the risk management, there should be a rule engine that will operate on user created command, access to data and to process it. As presented below in Figure 9 (Brad Calder,2003), risk management systems should have at least two features, risk reporting and monitoring module and risk modeling module the latter is especially important for "Financial Risk Management" modeling.

Figure 9
Sample Overview for an Enterprise Risk Management System



Source: Brad Calder,Stephen Elbert, Architecture and Performance of An Enterprise Desktop Grid System,2003.

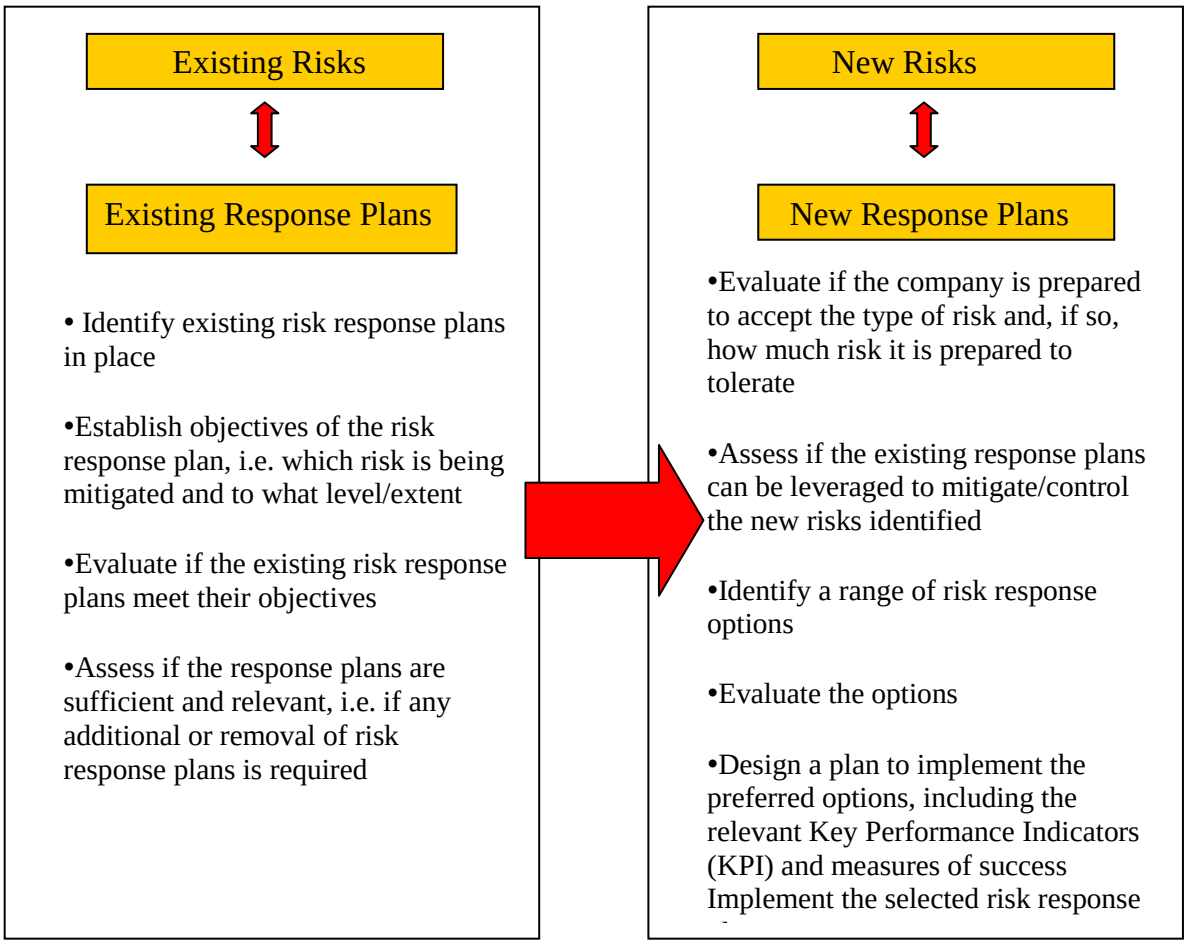
2.3.2.3.6. RISK MONITORING AND REPORTING

The monitoring and review of the risk profile and the risk response plans is a continuous process .The purpose of the review is to provide assurance that risks are being managed as expected, assess whether the risk response plans remain relevant and to ensure that the risk profile anticipates and reflects changed circumstances and new exposures.

Table 6 (Ahmet Uğur Cebeci, 2008) briefly summarizes the response alternatives for the existing and recently identified risks and suggestions of risk response plans.

Risk monitoring consists of a combination of regular communication, periodic reviews or audits and evaluation by independent executives at appropriate levels in a Telecommunication Company. Periodic review is important to the dynamics of the Telecommunication Industry as technology, customer needs and competitor's strategies have a tendency to shift frequently. Periodic review techniques can include the periodic or random testing of controls, risks and control environment, quality assurance reviews, post-implementation reviews and performance appraisals.

Table 7
Risk Response Plans



Source: Ahmet Uğur Cebeci, Işılda Arslan, Turkish Ministry of Finance, Chairmanship of Strategy Development, "Enterprise Risk Management,2008.

Risk response should be measured in terms of efficiency and effectiveness. Efficiency measures the cost of implementing risk management responses in terms of time, money and resources, whereas effectiveness measures the relative degree to which the responses reduce the impact or likelihood of the risk occurring. To maximize efficiency and

effectiveness of risk responses, monitoring and reporting should be integrated with existing business processes and reporting as far as possible.

While everyone in a Telecommunication Company is responsible for enterprise risk management up to certain degree and in their respective areas, some staff should have specific responsibilities. The policy, design and framework for enterprise risk management is driven by the Board and can be managed by the enterprise risk management team.

The reporting structure ensures that risk response gaps are addressed and the risk responses are operating effectively under changing conditions. Enterprise risk management activities should be monitored and reported upwards throughout in company as presented in the Figure 10 below (James Lam, 2004)

Figure 10

Risk Reporting Flow for a Telecommunication Company

Source: Lam James, Best Practices in KRI and ERM Reporting, 2004.

2.3.2.3.7. DESIGN ORGANIZATIONAL STRUCTURE ALTERNATIVES FOR RISK MANAGEMENT TEAMS

Even though Telecommunication Companies have complex organizational structures, operations and systems, it is not mandatory to have a Risk Committee (e.g. Turk Telekom) or separate Risk Management Department. It is important to ensure that risks are identified and managed. There are certain objectives required for the risk management organization structure, to support the organization's business objectives. These may include: Implementing risk management policies across all relevant business processes; Ensuring awareness of the risk management policies and procedures across the organization; Liasing with business segments regarding risk management process design, execution and ongoing assurance; Conducting risk-related due diligence on potential business partners and acquisitions; Monitoring compliance with the risk management policies and procedures; Providing a single point of focus internally and externally for risk-related issues; Representing the organization externally at key industry and advocacy groups; and Educating customers and suppliers about industry risk issues and the organization's Enterprise Risk Management Framework. Even though existing ERM structures differ from one Telecom company to another, there are three basic organizational structure alternatives for a Telecommunication Company.

- A Risk Management Department can be setup to co-ordinate all risk management activities throughout the organization. The Risk Management Department reports to a Chief Risk Officer role. Internal Audit is responsible for assessing the effectiveness of processes and testing the key controls and risk responses (James Lam, 2000);

- Risk Management Unit is setup; it is responsible for risk management assurance and compliance. This unit ensures that proper controls and risk responses are in place and completes the testing of these controls and responses. The combined unit reports

directly to the Risk and Audit Committee which should have an expanded scope for risk management activities (Raghunandan, K., 2001) and;

- Decentralized Risk Management structure is setup - risk management activities are embedded into the business processes and business units and functions are responsible for establishing risk management processes. Reporting of opportunities and risks to business objectives is through existing line management mechanisms Internal Audit's role continues to be one of assessing the efficiency and effectiveness of internal controls.

For each of the options, the organization structure, roles and responsibilities and reporting lines are described together with some potential strengths and weaknesses. These alternatives are only, they all assume that there exists an internal audit department/unit within the organization and act efficiently. Taking into consideration that all of the local Telecommunication Companies in Turkey such as; Turk Telecommunication, Avea, Turkcell and Vodafone have Internal Audit departments, organization alternatives above may suit them all. These alternatives do not represent a full set and are based around a given existing organization structure.

In determining an optimal risk management organization structure for a specific organization, a number of factors should be considering including: how risk management is to fit into the overall corporate objectives of the organization; the role that risk management is to play in the daily operational activities of the organization; the need to be able to balance the need for a strong control culture versus the flexibility to make quick and rapid business changes; the changes required of staff in terms of mindset, culture and behavior; and availability of suitable management resources.

3. THE RESEARCH METHODOLOGY

This is a descriptive study about how managers in telecommunication sector perceive Enterprise Risk Management Framework. There should be definitely further analysis and detailed research for detailed studies to understand correlations and factors.

Throughout the following section, the aim of the research study, the research sample selection, the research instrument and methodology is presented. In addition to this, survey questions that were issued to survey participants and survey results are presented as well, and then concluded with the analysis and the findings and final evaluation.

3.1 THE AIM OF THE RESEARCH

Before the survey questions were designed, I have interviewed senior management of another two major Telecom companies out of the four, in order to receive management insight regarding their both industrial and companywide risk management perspective and understanding. Per interview with senior management for those companies, I had received the information that all of them have a functioning Risk Management unit and had already started to embed risk management framework within their daily business operations. Depending on the companies' organizational behavior and cultural habits, the statements of the senior management were pretty optimistic and might be biased. Therefore, in order to analyze the maturity of existing risk management frameworks within Telecom companies, I selected a more scientific way; surveying.

The aim of the research was to have a broad understanding of the organizational structures of existing risk management functions such as how many people they deploy, for how long they work on risk management activities, the degree they embed their operations to daily business process of the company, not only from the perspective of risk managers or senior management but from the perspective of other critical units for risk management such as Sales& Marketing, Finance, Internal Audit, Strategic Planning, Legal and CHS

(Company Health and Safety) and Technical Departments etc as well. It is not wrong to assume the survey as a cross-check of the optimistic as-is scenarios presented by senior management of the interviewed companies.

3.2 THE RESEARCH SAMPLE AND PROCEDURE

The questionnaire was aimed to assess the maturity of the existing risk management functions within the big four Telecommunication companies of Turkish telecom market. These four companies represent the research universe rather than the research sample. During the selection of target audience for the survey, two factors were taken into consideration: one is distributing the survey between risk management specialist would result in receiving one way perspective and would not reflect the critical stakeholders within other departments as risk management is not only limited to risk management unit/department itself. Second: Risk management concept was limited to financial risk management and many companies did not have a solid understanding that enterprise wide risk management not only includes financial risk but also includes all types of risks at all business levels from high level strategic risks, investment risk to low level business process risks as well. Therefore different departments of Telecom companies and different level of management/specialist were included within the survey participants.

3.3 THE RESEARCH INSTRUMENT

The general methodology of this study relies largely on the survey questions which was issued to 200 employees of the big four Telecom companies within Turkey. The survey consisted of 62 questions of 6 of them are demographic questions aand 56 of them, mixed with a few different question techniques as matrix questions that participants are asked for their personal opinions/understandings, or multiple choice questions that participants can select only one answer mandatory or can select the applicable choices from the list below the question's body. A free text comment box for participant comments was not allowed in order to ease the analysis and evaluation of the survey results.

The survey was prepared in two formats, one was prepared in Microsoft Office Word and the other format was prepared as web-page. I had created a personal blog on blogspot.com (http://kurumsalriskyonetimi.blogspot.com/). Then I signed up for one of the famous free survey hosting web-sites : Polldaddy. I had published my survey questions electronically on this site and announced this site's survey links in my personal blog. I kept the participants free for choosing whether to fill the Word document or click on the links in my blog and directly filling the web-based survey form. There was a language barrier with some of the participants from two of the participant companies; therefore I chose to prepare the survey in Turkish which is also presented in next section below.

The survey questions were pilot tested with few of the participants beforehand for clarity, ease of use and value of the information that could be gathered. The initial survey which consisted of 98 questions was simplified and shortened to 62 questions. It was formulated by seeing the relevant literature in ERM in complex business environments such as banking, insurance and energy as well. In order to keep it easy for the participants, no complex calculations, financial figures or confidential information is requested. Even though few of the questions request numerical answers such as "How many employees does the Risk Management function has?", most of the questions are based on the cognitions and perceptions of the participants, the survey itself has a qualitative approach rather than quantitative approach.

3.4 SURVEY ANALYIS AND FINDINGS

As presented within the section 3.1 The Aim of The Research, the survey questions were issued to 200 employees of the four telecom companies in Turkey. Only 106 of those employees had completed the survey electronically on www.polldady.com electronically and rest of the 92 did not either responded or finished the survey completely. All of the 62 questions had been transferred to Microsoft Excel form polldaddy.com and imported into statistical analysis tool SPSS 18 for further review and analysis. As mentioned before, four of the companies that were selected for surveying represent the universe of "the telecom company set" in Turkey. While reviewing the survey findings below, it is important to keep in mind some background information of those companies. First of all, one of those telecom companies is semi-privatized telecom giant (55%) and 15% is traded in SPK, who still has nearly the 100% of the fixed line market with more than 29.000 employees. Taking into consideration that this company have different line of services to telecom customers, it bears a wider range of risks and strictly monitored by "Telekominikasyon Kurumu" when compared to remaining three. Also it is important to keep in mind that the corporate governance level and corporate culture is still carrying the influence of the days of being publicly owned. One of the other three companies is 81% of this formally mentioned telecom giant, so it is important to keep in mind that this company also is influenced by being publicly owned previously. Also it is obvious from the survey results that only the respondents from this second GSM company will state that the risk management activities are a part of the Holding company's risk management activities. One of the companies out of remaining two is the first Turkish GSM operator and it is not only traded in SPK but in New York Stock Exchange as well, therefore it is important to note that this company does not only obliged to comply with the risk management and corporate governance reporting of SPK but also obliged to comply with Sarbanes Oxley act too. Therefore it is not irrelevant to foresee that the respondents from this company will be more familiar with risk management, internal audit, risk monitoring and reporting concepts. The last company is an UK company, that is not publicly traded in Turkey. As it is also trade in

New York Stock Exchange, it is also obliged to obey to Sarbanes Oxley act as well as the previously mentioned one. Finally, all of these companies are externally audited by a professional audit company, and therefore all of them are using the COSO framework.

In light of these information, details of the survey analysis for each question with their brief review is explained in Appendix 6.2 Survey Results.

Table 8
Summary of the Descriptive Analyses of the Demographic Variables
(See Appendix 6.1 Questionnaire)

	Intervaş	**%**		
Age	30< yrs <40 yrs	88.7		
Tenure at Job	5< yrs < 20 yrs	67.2		
	Female	**Male**		
Gender	39	67		
	Married	**Single**		
Marital Status	60	46		
	High School	**University**	**Master D.**	**Doctorate**
Education	0	79	26	1
	Direktör	**Manager**	**Specialist**	**Other**
Statu	17	45	43	1

4. CONCLUSION

This study came out with a generic framework that can be utilized to address the issue of risk management for Telecommunication companies. There are quite a few conclusions that could be drawn from it. First conclusion is that, right risk management may vary from one firm to another based on the perception of risk in the corporate strategy and highly effected with the size of the firm and complexity of its business transactions and corporate culture. Secondly, an efficient risk management process is a slow process that has to create a common language, syntax and process to build capabilities at the pragmatic layer. Even though there are risk management practices in place, risk management approach should flow both from top to bottom and bottom to top between all levels. This process should especially be supported by top down strategic approach where ideally a corporate risk committee ensures the bottom-up's integration is happening in accordance with needs, requirement and corporate risk strategy of the firm. Although risk management is treated in a generic way across the firm, risk analysis and boundaries part of the process should be customized for each business function due to the complexity of the transactions and underlying systems in Telecommunication companies. Thirdly, a firm needs to manage the right amount of risk, no more, no less; therefore a thorough risk management need analysis is required before a firm decides to reach to highest bracket of risk management curve in the shortest amount of time.

I believe that this study was able to present the level of risk management maturity within Turkish telecom market. Its rationale was not only to provide a generic guideline for efficient implementation but also examined the existing point of view of the effected stakeholders within these companies by utilizing the survey. It is certain that organizations that are able to manage risks within their risk appetite and provide reasonable assurance to their stakeholders regarding the achievement of the organization's objectives will be the winners of the future.

5. REFERENCES

- Adrian R. Bowden,Malcolm R. Lane,Julia H. Martin Triple Bottomline Risk Management, 2001 pg 15-17.

- Ahmet Uğur Cebeci, Işılda Arslan, Turkish Ministry of Finance, Chairmanship of Strategy Development, "Enterprise Risk Management" pg 52-55, 62-67,70-84;

- A.Scott,, Risk Management Frameworks Institute of Internal Auditors Magazine, May 2004

- Banham, R. (2004), Enterprising views of risk management. Journal of Accountancy,197, 6, pp. 6571

- Barton, Thomas L., William G. Shenkir, and Paul L. Walker, Making Enterprise Risk Management Pay Off: How Leading Companies implement Risk Management, Financial Times/ Prentice Hall PTR (2002).

- Beasley, M.S., Carcello, J.V., & Hermanson, D.R. (1999), Fraudulent Financial Reporting: 19871997

- Beasley, Mark S., Clune, Richard, and Hermanson, Dana R., 2005, Enterprise risk management: An empirical analysis of factors associated with the extent of implementation, Journal of Accounting and Public Policy, 24, 521-31

- Beasley, Mark S., Pagach, Don, and Warr, Richard, 2006, The Information Conveyed in Hiring Announcements of Senior Executives Overseeing Enterprise-Wide Risk Management Processes, Working Paper, North Carolina State University.

- Beecheer Carlson, Transformational Change Reshapes What You Need in Telecommunications Risk Management, 2010, pg.11

- Bradly T. Borden, "Residual Risk Classification Model", 2010, pg 23.

- Brad Calder,Stephen Elbert, Architecture and Performance of An Enterprise Desktop Grid System,2003,pg 61

- Carcello, J.V., Hermanson, D.R., & Raghunandan, K. (2005), Factors associated with U.S. public companies' investment in internal auditing. Accounting Horizons, 19,2, pp. 6984. 21

- Committee of Sponsoring Organizations, Enterprise Risk Management Integrated Framework, Executive Summary, 2004, Foreword pg v and pg 5.

- Colquitt, L.L., Hoyt, R.E. & Lee, R.B. (1999), Integrated risk management and the role of the risk manager. Risk Management and Telecom Review, 2, pp. 4361.

- Earnst and Young, Oxford Analytica, Telecommunication Business Risk Report, 2009, pg 12

- Gramling, A.A., & Myers, P. (2006), The role of the internal audit function in enterprise-wide risk management. Working paper pg 21.

- Gwendal Le Grand, Eyal Adar, A Risk Assessment Tool for Network Resillience Evaluation, (2007), pg 11.

- Institute of Internal Auditors, Internal Auditor's Manual, Role of Internal Auditor in Risk Management, Section 4000-4100, 2008, pg 91-92.

- ITU World Telecommunication, Information and Telecommunication Indicators Database, Facts and Figures Report (2009), 13th Edition, pg 1-8.

- Kent D. Miller, Journal of International Business Studies, "A Framework for Integrated Risk Management in International Business", (1992) ,pg 311-315.

- Kimbrough, R L,Componation, P J, Relationship Between Risk Management and Organizational Culture, Engineering Management Journal, 2009.

- Kleffner, A., Lee, R., & McGannon, B. (2003), The effect of corporate governance on the use of enterprise risk management: Evidence from Canada. Risk Management and Insurance Review, 6, 1, pp. 5373.

- Lam James, Enterprise wide Risk Management and the Role of the Chief Risk Officer. ERisk, March 25, pp. 15. 22

- Lam James, Best Practices in KRI and ERM Reporting, 2004, pg 10-11

- Lam, James, Enterprise Risk Management: From Incentives to Controls, John Wiley & Sons, Inc. (2003)

- Miccolis, Jerry A., Kevin Hively, and Brian W. Merkley, Enterprise Risk Management: Trends and Emerging Practices, The Institute of Internal Auditors Research Foundation (2001).

- Miccolis, J., & Shah, S. (2001). Risk Value Insights: Creating value through enterprise risk management - A practical approach for the insurance industry.: Tillinghast-TowersPerrin Monograph.

- Michael Muehlen, Danny Ting Yi Ho, "Risk Management in the Business Process Management Lifecycle", 2005, pg 473

- Michel Crouhy, Dan Galai, Robert Mark, The Essentials of Risk Management, 2005, Chapter 2, pg 36

- Mittelstaedt, Robert E., Jr., Will Your Next Mistake be Fatal? Avoiding the Chain of Mistakes that can Destroy Your Organization, Wharton School Publishing (2005)

- Perrin. (2009), Enterprise Risk Management: Trends and Emerging Practices, Altamonte Springs, FL, Institute of Internal Auditors Research Foundation.

- PricewaterhouseCoopers, Management Barometer ERM Survey, (2007), Appendix 11.

- PricewaterhouseCoopers, Risk Scaling Methodology, 2004, pg 34

- Raghunandan, K., Read, W.J., & Rama, D.V. (2001), Audit committee characteristics, 'gray' directors, and interaction with internal auditing. Accounting Horizons, 15, June, pp. 105118.

- R Gregory, S Lichtenstein, A Hint of Risk: Tradeoffs Between Quantitative and Qualitative Risk Factors - Risk Analysis, 2006, pg 21.

- Richard Clune, Enterprise risk management: "An empirical analysis of factors associated with the extent of implementation" pg 13-15

- Richard.Clune, & Hermanson, D.R. (2005a), ERM: A status report. Internal Auditor, February, pp. 6772.

- Robert Philips, The Canadian Institute of Actuaries, Beyond Risk Magazine "A New Approach for Managing Operational Risks", 2008, pg 7

- Robert R Moeller, "Understanding the New Integrated COSO Integrated Framework" 2007, pg 41-42

- Rolf Olsson, International Journal of Project Management "Is The Risk Management Process Enough?", 2007, pg 745-752

- Scarbrough, P., Rama, D.V., & Raghunandan, K. (1998), Audit committees' interaction with internal auditing: Canadian evidence. Accounting Horizons, 12, March, 5162.

- The Committee of Sponsoring Organizations, ERM Integrated Framework, 2004, pg 8.

- The Conference Board, "Enterprise Risk Management: Managing the Cultural Change," The Conference Board (May, 2005.

- Tim Leech J., "The Next Wave in Assurance Thinking," Internal Auditor (August, 2000), pp. 66-71.

- Tim Leech, “How Do You Know If Risk Management Processes are Effective”, Institute of Internal Auditors Magazine, Dec 2009, pg 18.

- Walker, P.L., Shenkir, W.G., & Barton, T.L. (2002), Enterprise Risk Management: Putting it all Together

- World Intellectual Property Organization, Risk Assessment Methodology, 2004, pg 11-12.

- Vicky Arnold, Tanya Benford, Joseph Canada, Steve G. Sutton, “The Role of Enterprise Risk Management and Organizational Strategic Flexibility in Easing New Regulatory Compliance”, 2009, pg 11-13.

6. APPENDIX

6.1 QUESTIONNAIRE

Demographic Questions :

Soru 01. Lütfen yaşınızı seçiniz

□31- 35 arası
□36- 40 arası
□41- 50 arası
□51- üstü

Soru 02. Lütfen cinsiyetinizi seçiniz

□ Erkek
□ Kadın

Soru 03. Lütfen medeni durumunuzu seçiniz

□ Bekar
□ Evli

Soru 04. Lütfen eğitim durumunuzu seçiniz

□ İlköğretim
□ Lise
□ Meslek Lisesi
□ Üniversite
□ Lisans Üstü
□ Doktora

Soru 05. Kaç yıldır profesyonel olarak çalışmaktasınız?

□ 1-4
□ 5-9
□ 10-14
□ 15-19
□ 20-24
□ 25 ve üstü

Soru 06. Lütfen iş yerindeki statünüzü seçiniz

 Genel Müdür
 Genel Müdür Yardımcısı / Direktör
 Müdür
 Uzman
 Diğer

Survey Questions :

Soru 1- İşletmeniz kaç yıldır faaliyetlerini sürdürmektedir?

□ 5'ten az
□ 5-9 yıl arası
□ 10-19 yıl arası
□ 20 ve üstü

Soru 2- İşletmenizde kaç kişi istihdam edilmektedir?

□ 500'den az
□ 500-900 arası
□ 1000-1900 arası
□ 2000 ve üstü

Soru 3. İşletmenizde Risk Yönetim uygulaması var mıdır?

VAR □ YOK □

Soru 4. Risk yönetimi uygulamalarınız temel olarak hangi birimin sorumluluğu altındadır;

□ İç Denetim Birimi
□ Risk Yönetimi Birimi
□ Stratejik Yönetim
□ Finans
□ Planlama

Soru 5. Eğer Holding'e bağlı bir işletme iseniz Risk Yönetim uygulamanız holding'e bağlı mı yoksa ana şirket
faaliyeti olarak mı yürütülmektedir?

□ Holding'e bağlı

□ Ana Şirket Faaliyeti

Soru 6'dan soru 8'e kadar aşağıdaki skalaya göre işaretleyerek cevap veriniz.

Kesinlikle katılıyorum (5)
Katılıyorum (4)
Kararsızım (3)
Katılmıyorum (2)
Kesinlikle katılmıyorum (1)

Soru 6	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Risk yönetimi faaliyetlerimiz tamamen yerleşik ve iş süreçleri ile entegre durumdadır					

Soru 7	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Risk yönetimi faaliyetlerimiz kısmen yerleşik durumdadır fakat iş süreçlerine entegre edilmesi planlanmaktadır					

Soru 8	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Risk yönetimi faaliyetlerimiz Finans, İç Denetim vb alanlarla sınırlı kalmaktadır, tüm iş süreçleri ile entegre edilmesi konusunda üst yönetim tarafından henüz bir karar alınmamıştır.					

Soru 9. Risk Yönetim uygulamasına ne kadar süre önce başladınız?

□ 1 yıldan az
□ 1-4 yıl
□ 5-9 yıl
□ 10 ve üstü

Soru 10'dan soru 17'ye kadar aşağıdaki skalaya göre işaretleyerek cevap veriniz.

Kesinlikle katılıyorum (5)
Katılıyorum (4)
Kararsızım (3)
Katılmıyorum (2)
Kesinlikle katılmıyorum (1)

Soru 10	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirketimiz risk yönetimi faaliyetine yasal zorunluluklar sebebiyle geçmiştir					

Soru 11	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirketimiz risk yönetimi faaliyetine daha etkin iç denetim ve kontrol ihtiyacı sebebiyle geçmiştir					

Soru 12	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirketimiz risk yönetimi faaliyetine performans eksikliği, operasyonların verimliliğinin ve sürekliliğinin sağlanması sebebiyle geçmiştir					

Soru 13	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirketimiz risk yönetimi faaliyetine rekabet baskılarının artması sebebiyle geçmiştir					

Soru 14	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirketimiz risk yönetimi faaliyetine artan kriz frekansı, uygun bir kriz yönetimi ile krizlerin atlatılması sebebiyle geçmiştir					

Soru 15	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirketimiz risk yönetimi faaliyetine kurumun stratejisini etkileyebilecek potansiyel olayların belirlenmesi, yönetilmesi ve kurumun hedeflerine ulaşılmasının sağlanması ihtiyacı sebebiyle geçmiştir					
Soru 16	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirketimiz risk yönetimi faaliyetine finansal risklere karşı korunma ve finansal değişikliklerden faydalanma ihtiyacı sebebiyle					

geçmiştir					

Soru 17. İç kontrol ve Risk Yönetimi fonksiyonlarını yürütmekte olan birimlerin toplam eleman sayıları kaçtır?

□ 1-3
□ 4-6
□ 7-9
□ 10 ve üstü

Soru 18. Risk Yönetimi ve İç Denetim çalışanlarının bilgi ve becerilerini artırmaya yönelik yapılan eğitimler
veya eğitim planları var mı?

□VAR □YOK

Risk raporlama sisteminiz var ise, aşağıdaki skalayı kullanarak 19. soru ile devam ediniz, yok ise 24.soruya geçiniz)

Kesinlikle katılıyorum (5)
Katılıyorum (4)
Kararsızım (3)
Katılmıyorum (2)
Kesinlikle katılmıyorum (1)

Soru 19	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Risk raporlaması "Üst Yönetim"e yapılmaktadır					
Soru 20	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Risk raporlaması "Yönetim Kurulu"na yapılmaktadır					

Soru 21	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Risk raporlaması "Paydaşlar"a					

yapılmaktadır					
Soru 22	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Risk raporlaması "Tüm Şirket"e yapılmaktadır					

Soru 23	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Risk raporlaması "Yasal ve Düzenleyici Kurumlar"a yapılmaktadır					

Soru 24. İşletmeniz belirlediği ve bildirdiği bir risk yönetim tüzüğü (Risk Yönetiminin amaçlarını ve
taahhütlerini belirleyen resmi doküman) var mıdır? Var ise; bu tüzüğünüz şirketin tüm çalışanlarına bildirilmiş midir ?

 Risk yönetim tüzüğü mevcuttur ve şirket çalışanlarına bildirilmiştir
 Risk yönetim tüzüğü mevcuttur fakat şirket çalışanlarına bildirilmemiştir
 Risk yönetim tüzüğü mevcut değildir

Risk yönetimi faaliyetlerinin şirket içi diğer faaliyetlerle entegrasyonunu değerlendirmek amacıyla

25.sorudan 30.soruya kadar aşağıdaki skalayı kullanarak cevaplayınız.

Kesinlikle katılıyorum (5)
Katılıyorum (4)
Kararsızım (3)
Katılmıyorum (2)
Kesinlikle katılmıyorum (1)

Soru 25	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Kurum çapında riskleri değerlendirme faaliyeti şirketin iş uygulamalarına yerleşmiş ve/veya etkin ve efektif olarak yürütülmektedir					

Soru 26	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Risk yönetim pratiklerini geliştirmek için tavsiye ve öneriler verme faaliyeti şirketin iş uygulamalarına yerleşmiş ve/veya etkin ve efektif olarak yürütülmektedir					

Soru 27	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Bir risk yönetim raporlaması ve bilgi sistemi kurma faaliyeti şirketin iş uygulamalarına yerleşmiş ve/veya etkin ve efektif olarak yürütülmektedir					

Soru 28	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Kurum çapında risklerin kontrol aktiviteleri işletme faaliyeti şirketin iş uygulamalarına yerleşmiş ve/veya etkin ve efektif olarak yürütülmektedir					

Soru 29	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Kurum çapında risklerin takip edilmesi faaliyeti şirketin iş uygulamalarına yerleşmiş ve/veya etkin ve efektif olarak yürütülmektedir					

Soru 30. İşletmenizde risklerin belirlenmesi ve ölçülmesi için aşağıdaki yöntemlerden hangilerini
kullanıyorsunuz?

□ Temel performans göstergeleri
□ Temel risk göstergeleri
□ İç değerlendirme
□ Risk haritaları (belirleme, tanımlama ve önceliklendirme)
□ Sayısal yöntemler (VaR, Monte Carlo, vb.)
□ Diğer

Soru 31. Risk Haritalandırma var ise, ne sıklıkta yapılmakta? (Risk Haritalandırma yapmıyorsanız 25 soru ile devam ediniz)

□ Yılda Bir

□ Üç Ayda Bir
□ Ayda Bir
□ Sadece gerektiğinde
□ Risk haritalandırması yapmıyoruz

Soru 32. Hangi risk grubuna daha çok odaklanmaktasınız ? (Odaklanma sıranıza göre numaralandırabilirsiniz)

□ Finansal
□ Stratejik
□ Operasyonel
□ Çevre
□ Tümüne eşit odaklanırız

Soru 33. Kurumsal risk yönetimi konusunda şirket genelinde hangi standartları uyguluyorsunuz?

□ COSO
□ Australian Standard (AS / NZS 4360)
□ EU 8. Direktifi
□ Risk Management Standard (Risk Yönetimi Standardı)
□ Sarbanes-Oxley
□ The combined code on corporate governance (Kurumsal Yönetişim Bütünleşik Kuralları)
□ Basel II
□ OECD Kurumsal Yönetişim İlkeleri
□ Özel bir standart uygulamıyoruz

Soru 34. Hedeflediğiniz Risk Yönetimi ile şu an uygulamakta olduğunuz risk yönetim arasında fark var mıdır ?

EVET □ HAYIR □

Soru 35. Risk Yönetimi, kurumun hedeflerine ulaşma derecesini, faaliyetlerini ve geçmiş performansını ne
sıklıkta gözden geçirmektedir?"

□ Yılda Bir
□ Altı Ayda Bir
□ Üç Ayda Bir
□ Ayda Bir
□ Üst yönetim tarafından talep edildiğinde

Soru 36. Risk Yönetimi konusunda harici bir danışmanlık hizmeti almakta mısınız?

EVET □ HAYIR □

Soru 37. Bir dış denetçi (Kpmg, Ernest&Young, Deloitte, PwC vs…) ile çalışıyor musunuz?

EVET □ HAYIR □

Soru 38. İç Denetim ile ilgili, risk komitesinde yer alabilecek üst düzey kişiler var mıdır?

VAR □ YOK □

Soru 39. İç Denetim etkinliğini değerlendirmede en önemli kriteriniz nedir?

□ İç denetimlerin iç denetim raporuna uygun olarak tamamlanması
□ İç denetim raporlarının ne kadar sürede hazırlandığı
□ İç denetim planı kapsamındaki denetimleri zamanında tamamlayabilme
□ Denetim bulgularına istinaden, bulguların kapatılması için üst yönetime öneriler getirebilme

Soru 40. Uygulamada iç denetimin hangi işlevleri ön plana çıkmaktadır?

□Danışmanlık
□Uygunluk Denetim
□Güvence
□İş / Süreç Geliştirme
□Finansal Denetimi
□Faaliyet Denetimi
□Risk Yönetimi

Risk yönetimi faaliyetlerinin şirketinize katkısını değerlendirmek için, 41.sorudan 51.soruya kadar aşağıdaki skalayı kullanarak cevaplayınız.

Kesinlikle katılıyorum (5)
Katılıyorum (4)
Kararsızım (3)
Katılmıyorum (2)
Kesinlikle katılmıyorum (1)

Soru 41	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, sadece değer yaratacak risklerin alınmasını sağlamasıdır					

Soru 42	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, stratejik hedeflere ulaşılmasını sağlamasıdır					

Soru 43	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, yeni pazarlara girilmesini sağlamasıdır					

Soru 44	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, karlılığın artmasıdır					

Soru 45	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, rekabet gücünün artmasıdır					

Soru 46	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, yasal ve idari düzenlemelere uyum sağlanmasıdır					

Soru 47	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, düzgün kurumsal yönetim prosedürlerinin oluşturulmasıdır					

Soru 48	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, paydaşlara / hissedarlara doğru ve zamanında bilgi aktarımının sağlanmasıdır					

Soru 49	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, kurumun performansının izlenebilir hale gelmesidir					

Soru 50	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, karar mekanizmalarının ve iletişim ağlarının netleşmesidir					

Soru 51	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, etkin bir AR-GE yapısının kurulması ve işletilmesine imkan vermesidir					

Risk Yönetimini faaliyetlerinizi işletmenize yerleştirirken karşılaştığınız zorlukları değerlendirmek için, **52.sorudan itibaren aşağıdaki skalayı kullanarak cevaplayınız.**

Kesinlikle katılıyorum (5)
Katılıyorum (4)
Kararsızım (3)
Katılmıyorum (2)
Kesinlikle katılmıyorum (1)

Soru 52	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Risk Yönetimi sistemini kurmak ve faaliyetini sağlamaktaki en büyük engel, kurulum maliyetidir					

Soru 53	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Risk Yönetimi sistemini kurmak ve faaliyetini sağlamaktaki en büyük engel, kurumsallaşma eksikliğidir					

Soru 54	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Risk Yönetimi sistemini kurmak ve faaliyetini sağlamaktaki en büyük engel, devlet politikalarında ve ilgili düzenlemelerdeki değişikliklerdir					

Soru 55	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Risk Yönetimi sistemini kurmak ve faaliyetini sağlamaktaki en büyük engel, rakiplerin davranışları ve sektördeki sert rekabet koşullarıdır					

Soru 56	Kesinlikle katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle katılmıyorum
Risk Yönetimi sistemini kurmak ve faaliyetini sağlamaktaki en büyük engel, karmaşık iş süreçleri ve teknik altyapı eksiklikleridir					

6.2 SURVEY RESULTS

The responses to Survey Questions in addition to demographic variables of the research have been attached here with tables.

6.2.1 Demographic Analysis

The demographic variables of the study such as age, gender, marital status, education level, sector tenures and status of respondents at their job are examined respectively through frequency tables attached below.

Table 1 Frequency Distribution of Respondents' Age

D1Yas

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	30yas altı	25	23,6	23,6	23,6
	31-35 arası	28	26,4	26,4	50,0
	36-40 arası	41	38,7	38,7	88,7
	41-50 arası	9	8,5	8,5	97,2
	51yas ustı	3	2,8	2,8	100,0
	Total	106	100,0	100,0	

From the table, it can be inferred that 88.7% of the questionnaires have been answered by the employees below the age of 40. Among them, 36-40 years of age is 38.7% with the highest share followed by 31-35 years of age at 26.4% and younger than 30 years of age with 23.6% respectively.

Table 2 Frequency Distribution of Respondents' Gender

D2Cinsiyet

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Erkek	67	63,2	63,2	63,2
	Kadın	39	36,8	36,8	100,0
	Total	106	100,0	100,0	

63.2% of the questionnaires have been answered by male telecommunication sector respondents and 36.8% with femal ones.

Table 3 Frequency Distribution of Respondents' Marital Status

D3Medenidurum

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Evli	60	56,6	56,6	56,6
	Bekar	46	43,4	43,4	100,0
	Total	106	100,0	100,0	

56.6% of the questionnaires have been answered by married telecom professionals and 43.4% with single telecom professionals.

Table 4 Frequency Distribution of Respondents' Education Level

D4Egitim

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Üniversite	79	74,5	74,5	74,5
	Lisansüstü	26	24,5	24,5	99,1
	Doktora	1	,9	,9	100,0
	Total	106	100,0	100,0	

74.5% of the questionnaires have been answered by university graduate telecom professionals and 24.5% by telecom professionals with master degree.

Table 5 Frequency Distribution of Respondents' Tenure at Job

D5Kacyildircalisiyor

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-4 yil arasi	10	9,4	9,4	9,4
	5-9 yil arasi	34	32,1	32,1	41,5
	10-14 yil arasi	29	27,4	27,4	68,9
	15-19 yil arasi	29	27,4	27,4	96,2
	20-24 yil arasi	2	1,9	1,9	98,1
	25 yil ve üzeri	2	1,9	1,9	100,0
	Total	106	100,0	100,0	

92 respondents out of 106 with 86.9% have 5-20 years of job experience. 5-9 years has the highest amount at 32.1%. 10-14 years and 15-19 years have the second highest with 27.4% coming after.

Table 6 Frequency Distribution of Respondents' Statu at Job

D6Statü

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Direktör veya Genel Md. Yrd.	17	16,0	16,0	16,0
	Müdür	45	42,5	42,5	58,5
	Uzman	43	40,6	40,6	99,1
	Diğer	1	,9	,9	100,0
	Total	106	100,0	100,0	

16% of the questionnaires have been answered by Directors, 42.5% of the questionnaires have been answered by Manager level employees and 40.6% of the questionnaires have been answered by Specialist level telecommunication professionals.

6.2.2 Survey Analysis

The survey analysis of the study under 56 questions have been examined through frequency tables attached below.

Question 1 : İşletmeniz kaç yıldır faaliyetlerini sürdürmektedir?

Table 1 Frequency Distribution of Respondents' Companies' Operational Years

S1Faaliyetyili

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	5 den az	24	22,6	22,6	22,6
	5-10 yil arasi	23	21,7	21,7	44,3
	10-20 yil arasi	34	32,1	32,1	76,4
	20 yildan fazla	25	23,6	23,6	100,0
	Total	106	100,0	100,0	

Almost 77.4% of all participants have more than 5 years of job experience which is understandable since there is only one mobile operator company came to the country after 2005.

Question 2 : İşletmenizde kaç kişi istihdam edilmektedir?

Table 2 Frequency Distribution of Respondents' Companies' Employee Numbers

S2istihdamkisi

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2000 den fazla	106	100,0	100,0	100,0

100% of the participant to the survey have indicated that , their companies have more then 2000 employees which is absolutely logical considering the size of these companies

Question 3 : İşletmenizde Risk Yönetim uygulaması var mıdır?

Table 3 Frequency Distribution of Respondents' Answer to Risk Management in their Companies

S3riskyönuygl

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	var	105	99,1	99,1	99,1
	yok	1	,9	,9	100,0
	Total	106	100,0	100,0	

It has been seen that almost everyone said there is Risk Management approach in their companies.

Question 4 : Risk yönetimi uygulamalarınız temel olarak hangi birimin sorumluluğu altındadır ?

Table 4 Frequency Distribution of Respondents' which department/divison is responsible for Risk Management

S4hangibirimsorumlu

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	İç Denetim Birimi	59	55,7	55,7	55,7
	Risk Yönetim Birimi	45	42,5	42,5	98,1
	Finans	2	1,9	1,9	100,0
	Total	106	100,0	100,0	

It is good to hear that 42.5% , almost half of the participants have answered that 'Risk Management Divison' is responsible from managing the risks in their companies, led by the majority, 55.7% still saying that 'Internal Audit Division' of their companies is responsible for the Risk Management.

Question 5 : Eğer Holding'e bağlı bir işletme iseniz Risk Yönetim uygulamanız holding'e bağlı mı yoksa ana şirket faaliyeti olarak mı yürütülmektedir?

Table 5 Frequency Distribution of Respondents' whether Risk Management is a 'main company or holding center ' activity

S5şirketfaaliyeti

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	holding e bagli	19	17,9	17,9	17,9
	ana şirket faaliyeti	87	82,1	82,1	100,0
	Total	106	100,0	100,0	

It has been understood that Risk Management is a 'Main Company activity ' by 82.1%. The rest believes it has been held as a 'Holding Company's' responsibility and authority to manage the risks.

Question 6 : Risk yönetimi faaliyetlerimiz tamamen yerleşik ve iş süreçleri ile entegre durumdadır

Table 6 Frequency Distribution of Respondents' to Risk Management is in place and integrated with company's work processes

S6riskyönyerleşikentegre

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kesinlikle katılıyorum	12	11,3	11,3	11,3
	katılıyorum	75	70,8	70,8	82,1
	kararsızım	18	17,0	17,0	99,1
	kesinlikle katılmıyorum	1	,9	,9	100,0
	Total	106	100,0	100,0	

70.8% of the questionnaires have been answered as “agree” to the question 6. 17.0% of the respondents have answered as “not sure” and 11.3% of the respondents have answered as “definitely agree”.

Question 7 : Risk yönetimi faaliyetlerimiz kısmen yerleşik durumdadır fakat iş süreçlerine entegre edilmesi planlanmaktadır

Table 7 Frequency Distribution of Respondents’ to Risk Management is in place but integration with company’s work processes is planned

S7kismenyerlesikplanlı

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	7	6,6	6,6	6,6
	kararsızım	28	26,4	26,4	33,0
	katılmıyorum	59	55,7	55,7	88,7
	kesinlikle katılmıyorum	12	11,3	11,3	100,0
	Total	106	100,0	100,0	

55.7% of the questionnaires have been answered as “do not agree”. 26.4% of the respondents have answered as “not sure” , 11.3% said ‘I definitely and 6.6% of the respondents have answered as “definitely agree”.

Question 8 : Risk yönetimi faaliyetlerimiz Finans, İç Denetim vb alanlarla sınırlı kalmaktadır, tüm iş süreçleri ile entegre edilmesi konusunda üst yönetim tarafından henüz bir karar alınmamıştır.

Table 8 Frequency Distribution of Respondents’ to ‘Risk Management is only limited to Finance, Internal Audit etc. No decision taken by top management to integrate with company’s work processes ‘

S8finansicdenetimilesinirli

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kesinlikle katılıyorum	4	3,8	3,8	3,8
	katılıyorum	35	33,0	33,0	36,8
	kararsızım	39	36,8	36,8	73,6
	katılmıyorum	28	26,4	26,4	100,0
	Total	106	100,0	100,0	

36.58% of the questionnaires have been answered as “not sure” to the question. 33.0% of the respondents have answered as “agree’ and 26.4% of the respondents have answered as “donot agree” to the question 8.

Question 9 : Risk Yönetim uygulamasına ne kadar süre önce başladınız?

Table 9 Frequency Distribution of Respondents’ Period of Risk Management Application

S9kacyilöncebasladı

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 yıldan az	22	20,8	20,8	20,8
	1-5 yıl	83	78,3	78,3	99,1
	10 yil üzeri	1	,9	,9	100,0
	Total	106	100,0	100,0	

78.3% of the participants have indicated that they have started Risk Management 1-5 years ago.

Question 10: Şirketimiz risk yönetimi faaliyetine yasal zorunluluklar sebebiyle geçmiştir

Table 10 Frequency Distribution of Respondents' Risk Management is due to legally necessity

S10yasalzorunluluk

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	38	35,8	35,8	35,8
	kararsızım	41	38,7	38,7	74,5
	katılmıyorum	25	23,6	23,6	98,1
	kesinlikle katılmıyorum	2	1,9	1,9	100,0
	Total	106	100,0	100,0	

38.7% of the participants have answered as "not sure" to the question 10. Among 106 respondents , 35.8% have answered as "agree" and 23.6% of the respondents have answered as "not agree" to the question 10.

Question 11 : Şirketimiz risk yönetimi faaliyetine daha etkin iç denetim ve kontrol ihtiyacı sebebiyle geçmiştir

Table 11 Frequency Distribution of Respondents' to Risk Management is in place due to better 'Internal Audit and Control' necessity

S11dahaetkinicdenetim

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kesinlikle katılıyorum	9	8,5	8,5	8,5
	katılıyorum	13	12,3	12,3	20,8
	kararsızım	22	20,8	20,8	41,5
	katılmıyorum	62	58,5	58,5	100,0
	Total	106	100,0	100,0	

58.5 % of the questionnaires have been answered as “do not agree” to the question. 20.8% of the respondents have answered as “not sure’ and 12.3% of the respondents have answered as “agree” to the question 11.

Question 12 : Şirketimiz risk yönetimi faaliyetine performans eksikliği, operasyonların verimliliğinin ve sürekliliğinin sağlanması sebebiyle geçmiştir

Table 12 Frequency Distribution of Respondents’ to Risk Management to reach targeted performance level , efficiency and the continuity of the operations

S12iyiperformansopersverimliligi

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kararsızım	30	28,3	28,3	28,3
	katılmıyorum	76	71,7	71,7	100,0
	Total	106	100,0	100,0	

71.7 % of the questionnaires have been answered as “do not agree” to the question. 28.3% of the respondents have answered as “not sure’.

Question 13 : Şirketimiz risk yönetimi faaliyetine rekabet baskılarının artması sebebiyle geçmiştir

Table 13 Frequency Distribution of Respondents’ to Question Risk Management due to pressure by the competition

S13rekabetbaskısı

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kesinlikle katılıyorum	4	3,8	3,8	3,8
	katılıyorum	36	34,0	34,0	37,7
	Kararsızım	52	49,1	49,1	86,8
	katılmıyorum	13	12,3	12,3	99,1
	kesinlikle katılmıyorum	1	,9	,9	100,0

Question 14: Şirketimiz risk yönetimi faaliyetine artan kriz frekansı, uygun bir kriz yönetimi ile krizlerin atlatılması sebebiyle geçmiştir

Table 14 Frequency Distribution of Respondents' to Risk Management due to Economic Crisis

S14krizinatlatılması

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kesinlikle katılıyorum	32	30,2	30,2	30,2
	katılıyorum	54	50,9	50,9	81,1
	kararsızım	18	17,0	17,0	98,1
	katılmıyorum	2	1,9	1,9	100,0
	Total	106	100,0	100,0	

50.9 % of the questionnaires have been answered as "agree" to the question. 30.2% of the respondents have answered as "definitely agree" and 17.0% of the respondents have answered as "not sure " to the question 14.

Question 15: Şirketimiz risk yönetimi faaliyetine kurumun stratejisini etkileyebilecek potansiyel olayların belirlenmesi, yönetilmesi ve kurumun hedeflerine ulaşılmasının sağlanması ihtiyacı sebebiyle geçmiştir

Table 15 Frequency Distribution of Respondents' to Risk Management to clarify potential events (risks) that may affect the corporate strategy and targets

S15stratejiyietkilemek

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kesinlikle katılıyorum	12	11,3	11,3	11,3
	Katılıyorum	44	41,5	41,5	52,8
	Kararsızım	47	44,3	44,3	97,2
	Katılmıyorum	3	2,8	2,8	100,0
	Total	106	100,0	100,0	

44.3 % of the questionnaires have been answered as “not sure” to the question.. 2.8% of the respondents have answered as “definitely do not agree” and 41.5% of the respondents have answered as “agree” to the question 20 whereas still 11.3% said ‘definitely agree’

Question 16: Şirketimiz risk yönetimi faaliyetine finansal risklere karşı korunma ve finansal değişikliklerden faydalanma ihtiyacı sebebiyle geçmiştir

Table 16 Frequency Distribution of Respondents’ to Risk Management to protect against Financial Risks and Changes

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılmıyorum	77	72,6	72,6	72,6
	kesinlikle katılmıyorum	29	27,4	27,4	100,0
	Total	106	100,0	100,0	

72.6% of the questionnaires have been answered as “do not agree” to question 16, which is asking if the company had started risk management activities as a protection against financial risks and in order to benefit from financial changes/opportunities. 27.4% answered as “definitely do not agree” to the same question.

Question 17 :İç kontrol ve Risk Yönetimi fonksiyonlarını yürütmekte olan birimlerin toplam eleman sayıları kaçtır?

Table 17 Frequency Distribution of Respondents' Number of Employees in Risk Management Functions

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	6-10 kisi	48	45,3	45,3	45,3
	10 ve üzeri	58	54,7	54,7	100,0
	Total	106	100,0	100,0	

54.7% of the questionnaires have been answered that the total number of employees working in Internal Controls and Risk Management functions/departments are "more than 10 people". 45.3% of the questionnaires have been answered as "6-10 people" for the question 17.

Question 18: Risk Yönetimi ve İç Denetim çalışanlarının bilgi ve becerilerini artırmaya yönelik yapılan eğitimler veya eğitim planları var mı?

Table 18 Frequency Distribution of Respondents' Trainings and Trainings Plans

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	var	106	100,0	100,0	100,0

100% of the questionnaire have been answered that the companies all have trainings or future training plans to improve the capabilities of risk management and internal audit staff.

Question 19: Risk raporlaması "Üst Yönetim"e yapılmaktadır

Table 19 Frequency Distribution of Respondents' Risk Reported to Senior Management

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kesinlikle katılıyorum	3	2,8	2,8	2,8
	katılıyorum	1	,9	,9	3,8
	kararsızım	16	15,1	15,1	18,9
	katılmıyorum	66	62,3	62,3	81,1
	kesinlikle katılmıyorum	20	18,9	18,9	100,0
	Total	106	100,0	100,0	

62.3% of the questionnaires have been answered as "do not agree" to the question 19 that is asking if risks are reported to senior management. 18.9% of the respondents have answered as "definitely do not agree" and 15.1% of the respondents have answered as "not sure" to the question 19.

Question 20: Risk raporlaması "Yönetim Kurulu"na yapılmaktadır

Table 20 Frequency Distribution of Respondents' Risk Reported to Board of Directors

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kesinlikle katılıyorum	3	2,8	2,8	2,8
	Katılıyorum	13	12,3	12,3	15,1
	Kararsızım	8	7,5	7,5	22,6
	Katılmıyorum	67	63,2	63,2	85,8
	kesinlikle katılmıyorum	15	14,2	14,2	100,0
	Total	106	100,0	100,0	

63.2 % of the questionnaires have been answered as “do not agree” to the question 20 that is asking if risks are reported to board of directors. 14.2% of the respondents have answered as “definitely do not agree” and 12.3% of the respondents have answered as “agree” to the question 20.

Question 21: Risk raporlaması “Paydaşlar”a yapılmaktadır

Table 21 Frequency Distribution of Respondents’ Risk Reported to Shareholders

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	25	23,6	23,6	23,6
	kararsızım	39	36,8	36,8	60,4
	katılmıyorum	42	39,6	39,6	100,0
	Total	106	100,0	100,0	

39.6% of the questionnaires have been answered as “do not agree” to the question 21 that is asking if risks are reported to shareholders. 36.8% the respondents have answered as “not sure” and 23.6% of the respondents have answered as “agree” to the question 21.

Question 22: Risk raporlaması “Tüm Şirket”e yapılmaktadır

Table 22 Frequency Distribution of Respondents’ Risk Reported to Enterprise - Wide

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kesinlikle katılıyorum	24	22,6	22,6	22,6
	katılıyorum	69	65,1	65,1	87,7
	kararsızım	12	11,3	11,3	99,1
	katılmıyorum	1	,9	,9	100,0
	Total	106	100,0	100,0	

65.1% of the questionnaires have been answered as “agree” and 22.6% of them have been answered as “definitely agree” to the question 22 that is asking if risks are reported enterprise-wide. 11.3% the respondents have answered as “not sure” to the question 22.

Question 23: Risk raporlaması “Yasal ve Düzenleyici Kurumlar”a yapılmaktadır

Table 23 Frequency Distribution of Respondents’ Reporting done to Related Legal and Regulatory Bodies

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Katılıyorum	8	7,5	7,5	7,5
	Kararsızım	95	89,6	89,6	97,2
	Katılmıyorum	3	2,8	2,8	100,0
	Total	106	100,0	100,0	

89,6% of the questionnaires have been answered as “not sure” to question 23 which is asking if risk reporting is done to related legal and regulatory bodies. This result can be interpreted that either the majority of the respondents are not aware if their company reports risk management activities formally to “Telekominikasyon Kurumu”. 7,5% of the respondents answered as “agree” and 2.8% of the respondents answered as “do not agree” to question 23.

Question 24: İşletmeniz belirlediği ve bildirdiği bir risk yönetim tüzüğü (Risk Yönetiminin amaçlarını ve taahhütlerini belirleyen resmi doküman) var mıdır? Var ise; bu tüzüğünüz şirketin tüm çalışanlarına bildirilmiş midir?

Table 24 Frequency Distribution of Respondents' Risk Management Charter

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	risk yönetim tüzüğü mevcuttur ve şirket çalışanlarına bildirilmiştir	2	1,9	1,9	1,9
	risk yönetim tüzüğü mevcuttur fakat şirket çalışanlarına bildirilmemiştir.	78	73,6	73,6	75,5
	risk yönetim tüzüğü mevcut değildir	26	24,5	24,5	100,0
	Total	106	100,0	100,0	

73.6% of the questionnaires have been answered that risk management charter exists within their company but it is not formally shared with the employees. 24.5% of the respondents have answered that, their company do not have a risk management charter.

Question 25: Kurum çapında riskleri değerlendirme faaliyeti şirketin iş uygulamalarına yerleşmiş ve/veya etkin ve efektif olarak yürütülmektedir

Table 25 Frequency Distribution of Respondents' Risk Assessment Integrated to Business Processes and Operated Efficiently

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	73	68,9	68,9	68,9
	kararsızım	31	29,2	29,2	98,1
	katılmıyorum	1	,9	,9	99,1
	kesinlikle katılmıyorum	1	,9	,9	100,0
	Total	106	100,0	100,0	

68.9% of the questionnaires have been answered as “agree” to question 25 which is asking if risk assessment activities are integrated to business processes and operated efficiently. 29.2% of the respondents have answered as “not sure” and only total of 1.8 % of the respondents do not agree that risk assessment activities are integrated to business processes and operated efficiently.

Question 26: Risk yönetim pratiklerini geliştirmek için tavsiye ve öneriler verme faaliyeti şirketin iş uygulamalarına yerleşmiş ve/veya etkin ve efektif olarak yürütülmektedir.

Table 26 Frequency Distribution of Respondents’ Consulting on Developing Risk Panagement Practices Integrated to Business Processes and Operated Efficiently

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	41	38,7	38,7	38,7
	kararsızım	62	58,5	58,5	97,2
	katılmıyorum	3	2,8	2,8	100,0
	Total	106	100,0	100,0	

58.5% of the questionnaires have been answered as “not sure” to question 26 which is asking if activities of consulting on developing risk management practices are integrated to business processes and operated efficiently. 38.7% of the respondents have answered as “agree” and only 2.8% of the respondents have answered as “do not agree”.

Question 27: Bir risk yönetim raporlaması ve bilgi sistemi kurma faaliyeti şirketin iş uygulamalarına yerleşmiş ve/veya etkin ve efektif olarak yürütülmektedir

Table 27 Frequency Distribution of Respondents' Reporting and Related System Building Integrated to Business Processes and Operated Efficiently

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	62	58,5	58,5	58,5
	kararsızım	42	39,6	39,6	98,1
	katılmıyorum	2	1,9	1,9	100,0
	Total	106	100,0	100,0	

58.5% of the questionnaires have been answered as "agree" to question 27 which is asking if activities of risk reporting and related system building are integrated to business processes and operated efficiently. 39.6% of the respondents have answered as "not sure" and only 1.9% of the respondents have answered as "do not agree".

Question 28: Kurum çapında risklerin kontrol aktiviteleri işletme faaliyeti şirketin iş uygulamalarına yerleşmiş ve/veya etkin ve efektif olarak yürütülmektedir

Table 28 Frequency Distribution of Respondents' Enterprise Wide Risk-Control Integrated to Business Processes and Operated Efficiently

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	17	16,0	16,0	16,0
	kararsızım	66	62,3	62,3	78,3
	katılmıyorum	23	21,7	21,7	100,0
	Total	106	100,0	100,0	

62.3% of the questionnaires have been answered as “not sure” to question 28, which is asking if the enterprise wide risk-control activities are integrated to business processes and operated efficiently. 21.7% of the respondents have answered as “do not agree” and 16% of the respondents have answered as “agree” to the question 28.

Question 29: Kurum çapında risklerin takip edilmesi faaliyeti şirketin iş uygulamalarına yerleşmiş ve/veya etkin ve efektif olarak yürütülmektedir

Table 29 Frequency Distribution of Respondents’ Enterprise Wide Risk Monitoring Integrated to Business Processes and Operated Efficiently

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	31	29,2	29,2	29,2
	kararsızım	52	49,1	49,1	78,3
	katılmıyorum	23	21,7	21,7	100,0
	Total	106	100,0	100,0	

49.1% of the questionnaires have been answered as “not sure” to question 29, asking if the enterprise wide risk monitoring is integrated to business processes and operated efficiently. 29.2% of the respondents have answered as “agree” and 21.7% of the respondents have answered as “do not agree” to the same question.

Question 30: İşletmenizde risklerin belirlenmesi ve ölçülmesi için aşağıdaki yöntemlerden hangilerini kullanıyorsunuz?

Table 30 Frequency Distribution of Respondents’ Risk Evolution and Assessment

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	temel risk göstergeleri	1	,9	,9	,9
	iç değerlendirme	77	72,6	72,6	73,6
	risk hataları	28	26,4	26,4	100,0
	Total	106	100,0	100,0	

72.6% of the questionnaires have been answered that their company uses “internal evolution/assessment” for risk identification and measurement. 26.4% of the respondents have answered that their company uses “risk mapping” for risk identification and measurement.

Question 31: Risk Haritalandırma var ise, ne sıklıkta yapılmaktadır?

Table 31 Frequency Distribution of Respondents’ Frequency of Risk-Mapping

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	üç ayda bir	11	10,4	10,4	10,4
	altı ayda bir	2	1,9	1,9	12,3
	sadece gerektiğinde	93	87,7	87,7	100,0
	Total	106	100,0	100,0	

87.7% of the questionnaires have been answered that, the companies make risk mapping only “when needed”. 10.4% of the respondents have answered that their company makes risk mapping quarterly and only the 1.9% of the respondents have answered that their company makes risk mapping semi-annually.

Question 32: Hangi risk grubuna daha çok odaklanmaktasınız ?

Table 32 Frequency Distribution of Respondents’ Companies Mostly Focus

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	finansal	74	69,8	69,8	69,8
	stratejik	1	,9	,9	70,8
	operasyonel	22	20,8	20,8	91,5
	Tümüne eşit odaklanırız	9	8,5	8,5	100,0
	Total	106	100,0	100,0	

69.8% of the questionnaires have answered that the companies focus mostly on "financial risks", 20.8% of the respondents have answered that their company focuses mostly on "operational risks". Only 8.5% of the respondents have answered that their company focuses on each group of risk equally.

Question 33: Kurumsal risk yönetimi konusunda şirket genelinde hangi standartları uyguluyorsunuz?

Table 33 Frequency Distribution of Respondents' the Most Common Risk Management Framework Applied

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	COSO	58	54,7	54,7	54,7
	Sarbanes-Oxley	25	23,6	23,6	78,3
	Özel bir standart uygulamıyoruz	23	21,7	21,7	100,0
	Total	106	100,0	100,0	

54.7% of the questionnaires have been answered that the most common risk management framework applied in companies regarding risk management is the COSO framework. 23.6% of the respondents have answered that, their company applies Sarbanes Oxley requirements and 21.7% of the respondents have answered that their company does not apply as special framework regarding risk management.

Question 34: Hedeflediğiniz Risk Yönetimi ile şu an uygulamakta olduğunuz risk yönetim arasında fark var mıdır?

Table 34 Frequency Distribution of Respondents' Gap between the Targeted Risk Management and Existing Risk Management

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	evet	105	99,1	99,1	99,1
	hayır	1	,9	,9	100,0
	Total	106	100,0	100,0	

99.1% of the questionnaires have been answered as "Yes" to question 34, which asks if there is a gap between the targeted risk management and existing risk management application within the company.

Question 35: Risk Yönetimi, kurumun hedeflerine ulaşma derecesini, faaliyetlerini ve geçmiş performansını ne sıklıkta gözden geçirmektedir?

Table 35 Frequency Distribution of Respondents' Frequency of Reviewing the Company's Performance

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yılda bir	37	34,9	34,9	34,9
	altı ayda bir	59	55,7	55,7	90,6
	üç ayda bir	2	1,9	1,9	92,5
	Üst yönetim tarafından talep edildiğinde	8	7,5	7,5	100,0
	Total	106	100,0	100,0	

55.7% of the questionnaires have been answered as "semi-annually" to the question 35, which asks the frequency of reviewing the company's performance in meeting it's targets,

operations and it's performance history. 34.9% of the respondents have answered as "annually" to question 35.

Question 36: Risk Yönetimi konusunda harici bir danışmanlık hizmeti almakta mısınız?

Table 36 Frequency Distribution of Respondents' External Consultant Company

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	evet	104	98,1	98,1	98,1
	hayır	2	1,9	1,9	100,0
	Total	106	100,0	100,0	

98.1% of the questionnaires have been answered as "Yes" to the question 36, which asks if the company is receiving an external consulting service regarding risk management.

Question 37: Bir dış denetçi (Kpmg, Ernest&Young, Deloitte, PwC vs…) ile çalışıyor musunuz?

Table 37 Frequency Distribution of Respondents' External Audit Company

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	evet	105	99,1	99,1	99,1
	hayır	1	,9	,9	100,0
	Total	106	100,0	100,0	

99.1% of the questionnaires have been answered as "Yes" to question 37, which asks if the company is externally audited by an professional audit company.

Question 38: İç Denetim ile ilgili, risk komitesinde yer alabilecek üst düzey kişiler var mıdır ?

Table 38 Frequency Distribution of Respondents' Senior Executives who can represent Internal Audit in Risk Committee

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	var	81	76,4	76,4	76,4
	yok	25	23,6	23,6	100,0
	Total	106	100,0	100,0	

76.4% of the questionnaires have been answered that, there exists senior executives who can represent internal audit in Risk Committee. 23.6% of the questionnaires have been answered that, they do not have a senior executive regarding internal audit in Risk Committee.

Question 39: İç Denetim etkinliğini değerlendirmede en önemli kriteriniz nedir?

Table 39 Frequency Distribution of Respondents' the Most Important Criteria for Evaluating the Performance of Internal Audit

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	iç denetim raporlarının ne kadar sürede hazırlandığı	21	19,8	19,8	19,8
	iç denetim planı kapsamındaki denetimleri zamanında tamamlıyabilme	42	39,6	39,6	59,4
	Denetim bulgularına istinaden,bulguların kapatılması için üst yönetime öneriler getirebilme	43	40,6	40,6	100,0
	Total	106	100,0	100,0	

40.6% of the questionnaires have been answered that the most important criteria for evaluating the performance of internal audit is “the capability of internal audit to advise to senior management regarding the internal audit findings and how to take corrective actions to close those findings”. 39.6% of the respondents have answered that the most important criteria for evaluating the performance of internal audit is “the capability of internal audit to complete the audit plan on time as planned”. 19.8% of the respondents have answered that the most important criteria for evaluating the performance of internal audit is “internal audit’s efficiency of on time audit reporting”.

Question 40: Uygulamada iç denetimin hangi işlevleri ön plana çıkmaktadır

Table 40 Frequency Distribution of Respondents’ the Most Significant Function of Internal Audit

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Uygunluk Denetimi	21	19,8	19,8	19,8
	Güvence	2	1,9	1,9	21,7
	Finansal Denetim	23	21,7	21,7	43,4
	Faaliyet Denetimi	60	56,6	56,6	100,0
	Total	106	100,0	100,0	

56.6% of the questionnaires have been answered that the most significant function of internal audit is performing “operational audit”, 21.7% of the questionnaires have been answered as “financial audit” and 19.8% of the questionnaires have been answered as “compliance audit” to the question 40.

Question 41: Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, sadece değer yaratacak risklerin alınmasını sağlamasıdır

Table 41 Frequency Distribution of Respondents' Taking Risks Adding Value

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	40	37,7	37,7	37,7
	kararsızım	51	48,1	48,1	85,8
	katılmıyorum	14	13,2	13,2	99,1
	kesinlikle katılmıyorum	1	,9	,9	100,0
	Total	106	100,0	100,0	

48.1% of the questionnaires have been answered as "not sure" to question 41, which can be interpreted that, one of the most important benefits of effective risk management is, it enables the company to take only the risks that will add value. 37.7% of the respondents have answered as "agree" and 13.2% of the respondents have answered "do not agree" to question 41.

Question 42: Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, stratejik hedeflere ulaşılmasını sağlamasıdır

Table 42 Frequency Distribution of Respondents' to Meet its Strategic Goals and Targets

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	56	52,8	52,8	52,8
	kararsızım	47	44,3	44,3	97,2
	katılmıyorum	2	1,9	1,9	99,1
	kesinlikle katılmıyorum	1	,9	,9	100,0
	Total	106	100,0	100,0	

52.8% of the questionnaires have been answered as “agree” to question 42, which can be interpreted that one of the most important benefits of effective risk management is that it helps the company to meet its strategic goals and targets. 44.3% of the respondents have answered as “not sure” and total of 2.8 % of respondents do not agree that effective risk management has positive impact on meeting the strategic goals and targets.

Question 43: Şirket olarak Risk Yönetimi’nden sağladığımız en önemli fayda, yeni pazarlara girilmesini sağlamasıdır

Table 43 Frequency Distribution of Respondents’ Opportunity of Penetration to New Markets

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kesinlikle katılıyorum	19	17,9	17,9	17,9
	katılıyorum	49	46,2	46,2	64,2
	kararsızım	36	34,0	34,0	98,1
	katılmıyorum	1	,9	,9	99,1
	kesinlikle katılmıyorum	1	,9	,9	100,0
	Total	106	100,0	100,0	

46.2% of the questionnaires have been answered as “agree” and 17.9% of the questionnaires have been answered as “definitely agree” to the question 43, which can be interpreted that one of important benefits of effective risk management is the opportunity of penetration to new markets. 34% of the respondents have answered as “not sure” about the positive impact of risk management on market penetration.

Question 44: Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, karlılığın artmasıdır

Table 44 Frequency Distribution of Respondents' Increase on Profitability

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	61	57,5	57,5	57,5
	kararsızım	32	30,2	30,2	87,7
	katılmıyorum	13	12,3	12,3	100,0
	Total	106	100,0	100,0	

57.5% of the questionnaires have been answered to question 44, which can be interpreted that, the most important benefit of effective risk management is the increase in profitability. 30.2% of the respondents have answered as "not sure" and 12.3% of the respondents have answered as "do not agree".

Question 45: Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, rekabet gücünün artmasıdır

Table 45 Frequency Distribution of Respondents' Benefit of Increasing Competitve Edge

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	48	45,3	45,3	45,3
	kararsızım	54	50,9	50,9	96,2
	katılmıyorum	4	3,8	3,8	100,0
	Total	106	100,0	100,0	

50.9% of the questionnaires have been answered as “not sure” and 45.3% of the questionnaires have been answered as “agree”, to the question 45. Only 3.8% of the respondents have answered as”do not agree” to the most important benefit of effective risk management is the increase in competitive power/advantage.

Question 46: Şirket olarak Risk Yönetimi’nden sağladığımız en önemli fayda, yasal ve idari düzenlemelere uyum sağlanmasıdır

Table 46 Frequency Distribution of Respondents’ Compliance with Telecom Related Laws and Regulations

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kesinlikle katılıyorum	1	,9	,9	,9
	katılıyorum	10	9,4	9,4	10,4
	kararsızım	20	18,9	18,9	29,2
	katılmıyorum	71	67,0	67,0	96,2
	kesinlikle katılmıyorum	4	3,8	3,8	100,0
	Total	106	100,0	100,0	

67% of the questionnaires have been answered as “do not agree” to the question which can be interpreted as the majority of the respondents do not believe that effective risk management has positive impact on company’s compliance with telecom related laws and regulations. 18.9% of the questionnaires have been answered as “not sure” and only 9.4% of the questionnaires have been answered as “agree” to question 46.

Question 47: Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, düzgün kurumsal yönetim prosedürlerinin oluşturulmasıdır

Table 47 Frequency Distribution of Respondents' Proper Corporate Governance Procedures

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	1	,9	,9	,9
	kararsızım	33	31,1	31,1	32,1
	katılmıyorum	67	63,2	63,2	95,3
	kesinlikle katılmıyorum	5	4,7	4,7	100,0
	Total	106	100,0	100,0	

63.2% and 4.7% of the questionnaires, which totals to 67.9% have been answered "do not agree" and "definitely do not agree" respectively to question 47, which can be interpreted as, majority of the respondents do not believe that the most important benefit of effective risk management is creating proper corporate governance procedures.

Question 48: Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, paydaşlara / hissedarlara doğru ve zamanında bilgi aktarımının sağlanmasıdır

Table 48 Frequency Distribution of Respondents' Right and Timely Information Sharing to Shareholders

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	13	12,3	12,3	12,3
	kararsızım	82	77,4	77,4	89,6
	katılmıyorum	11	10,4	10,4	100,0
	Total	106	100,0	100,0	

77.4% of the questionnaires have been answered as “not sure” to question 48 which can be interpreted as, either the respondents are not sure about the relation or risk management with shareholder reporting or they are not informed about if risk management results are formally presented within the periodic shareholder report of their company. 12.3% answered as “agree” and 10.4% as not dot agree to the question 48.

Question 49: Şirket olarak Risk Yönetimi’nden sağladığımız en önemli fayda, kurumun performansının izlenebilir hale gelmesidir

Table 49 Frequency Distribution of Respondents’ Monitoring the Company’s Performance

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	2	1,9	1,9	1,9
	kararsızım	34	32,1	32,1	34,0
	katılmıyorum	70	66,0	66,0	100,0
	Total	106	100,0	100,0	

66% of the questionnaires have been answered as “do not agree” that risk management has positive impact on monitoring the company’s performance. 32.1% of the respondents have answered as “not sure” and only 1.9 percent believes that risk management is beneficial for performance monitoring.

Question 50: Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, karar mekanizmalarının ve iletişim ağlarının netleşmesidir

Table 50 Frequency Distribution of Respondents' Clarifying Decision Making Systems and Related Communication Networks within the Company

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kesinlikle katılıyorum	2	1,9	1,9	1,9
	Katılıyorum	9	8,5	8,5	10,4
	Kararsızım	49	46,2	46,2	56,6
	Katılmıyorum	46	43,4	43,4	100,0
	Total	106	100,0	100,0	

46.2% of the questionnaires have been answered as "not sure" regarding the positive effect of risk management on clarifying decision making systems and related communication networks within the company. 43.4 % of them responded as risk management is not a benefit factor for this clarification. Only total of 10.4% of the respondents agreed about the positive impact of risk management on decision making and internal communication networks.

Question 51: Şirket olarak Risk Yönetimi'nden sağladığımız en önemli fayda, etkin bir AR-GE yapısının kurulması ve işletilmesine imkan vermesidir

Table 51 Frequency Distribution of Respondents' Positive Impact on Set-Up and Operating an Effective R&D Framework

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kesinlikle katılıyorum	73	68,9	68,9	68,9
	Katılıyorum	31	29,2	29,2	98,1
	Katılmıyorum	1	,9	,9	99,1
	kesinlikle katılmıyorum	1	,9	,9	100,0
	Total	106	100,0	100,0	

68.9 % of the questionnaires have been answered as “definitely agree” and 29.2% of the questionnaires have been answered as “agree” to question 51, which can be interpreted as effective risk management has a positive impact on set up and operating an effective Research & Development framework.

Question 52: Risk Yönetimi sistemini kurmak ve faaliyetini sağlamaktaki en büyük engel, kurulum maliyetidir

Table 52 Frequency Distribution of Respondents’ Set-Up Cost as barrier for Implementing an Effective Enterprise Risk Management Framework

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	katılıyorum	12	11,3	11,3	11,3
	kararsızım	35	33,0	33,0	44,3
	katılmıyorum	59	55,7	55,7	100,0
	Total	106	100,0	100,0	

55.7% of the questionnaires have been answered as “do not agree” to the question 52, which means that majority of the respondents, do not believe that, set-up cost is a valid barrier for implementing an effective Enterprise Risk Management framework. 33 % of the respondents answered as “not sure” and only 11.3% of the respondents have answered as “agree.”

Question 53: Risk Yönetimi sistemini kurmak ve faaliyetini sağlamaktaki en büyük engel, kurumsallaşma eksikliğidir

Table 53 Frequency Distribution of Respondents' Corporate Culture as Effective Factor in Implanting Enterprise Risk Management Framework

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kesinlikle katılıyorum	1	,9	,9	,9
	Katılıyorum	18	17,0	17,0	17,9
	Kararsızım	27	25,5	25,5	43,4
	Katılmıyorum	36	34,0	34,0	77,4
	kesinlikle katılmıyorum	24	22,6	22,6	100,0
	Total	106	100,0	100,0	

34% of the questionnaires have been answered as "do not agree" and 22,6% have been answered as definitely do not agree which means that corporate governance or corporate culture is not a valid barrier for implementing and effective Enterprise Risk Management system. 25.5% of the respondents have answered as "not sure" to the same question and only total of 17.5% of the respondents have answered that corporate governance is an effective factor in implanting Enterprise Risk Management framework.

Question 54: Risk Yönetimi sistemini kurmak ve faaliyetini sağlamaktaki en büyük engel, devlet politikalarında ve ilgili düzenlemelerdeki değişikliklerdir

Table 54 Frequency Distribution of Respondents' Corporate Governance as an Effective Factor in Implanting Enterprise Risk Management Framework.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Katılıyorum	1	,9	,9	,9
	Kararsızım	27	25,5	25,5	26,4
	Katılmıyorum	61	57,5	57,5	84,0
	kesinlikle katılmıyorum	17	16,0	16,0	100,0
	Total	106	100,0	100,0	

57.5% and 16% of the questionnaires have been answered as “do not agree” and “definitely do not agree” respectively, which means the 93% of the respondents have answered that government policies and industry related regulations are not valid barriers for implementing an effective Enterprise Risk Management framework. It was also noted within this study that, even though Telecom industry is strictly regulated, these regulations promote the implementation of effective internal control and risk management systems, rather than being a barrier for implementation.

Question 55 : Risk Yönetimi sistemini kurmak ve faaliyetini sağlamaktaki en büyük engel, rakiplerin davranışları ve sektördeki sert rekabet koşullarıdır

Table 55 Frequency Distribution of Respondents’ Competition as barrier or Implementing an Effective Enterprise Risk Management Framework.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	kesinlikle katılıyorum	7	6,6	6,6	6,6
	katılıyorum	1	,9	,9	7,5
	kararsızım	85	80,2	80,2	87,7
	katılmıyorum	13	12,3	12,3	100,0
	Total	106	100,0	100,0	

80% of the questionnaires have been answered as “not sure” to the question 55 which asks if the competition in the telecom market is a valid barrier for implementing an effective Enterprise Risk Management framework. 27% of the questionnaires have been answered as definitely do not agree, and only 3.8 % of them have been answered as “agree” to question 55.

Question 56 : Risk Yönetimi sistemini kurmak ve faaliyetini sağlamaktaki en büyük engel, karmaşık iş süreçleri ve teknik altyapı eksiklikleridir

Table 56 Frequency Distribution of Respondents’ Complexity of the Business Processes and Deficiencies as barriers for Effective Implementation of Enterprise Risk Management Framework

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Katılıyorum	4	3,8	3,8	3,8
	Katılmıyorum	73	68,9	68,9	72,6
	kesinlikle katılmıyorum	29	27,4	27,4	100,0
	Total	106	100,0	100,0	

68.9% of the questionnaires have been answered as “do not agree” and 27.4% of the questionnaires have been answered as “definitely do not agree” by the respondents. Only 3.8% responded as “agree”. It is noted that, majority of the respondents do not believe that, complexity of the business processes and deficiencies in underlying systems are not valid barriers for effective implementation of Enterprise Risk Management framework